Kaspersky Internet Security 2012



BENUTZERHANDBUCH

PROGRAMMVERSION: 12.0

Sehr geehrter Benutzer!

Vielen Dank, dass Sie unser Produkt ausgewählt haben. Wir hoffen, dass diese Dokumentation Ihnen hilft und die meisten Fragen damit beantwortet werden können.

Kaspersky Lab behält sich das Recht vor, dieses Dokument ohne vorherige Benachrichtigung zu ändern. Die neueste Version finden Sie auf der Seite von Kaspersky Lab unter der Adresse http://www.kaspersky.de/docs.

Redaktionsdatum: 19.04.2011

www.kaspersky.de
http://support.kaspersky.de

INHALT

ÜBER DIESES HANDBUCH

Die Spezialisten von Kaspersky Lab begrüßen Sie herzlich.

Dieses Handbuch informiert über Installation, Konfiguration und Verwendung des Programms Kaspersky Internet Security. Wir hoffen, dass Ihnen dieses Handbuch bei der Arbeit mit dem Programm behilflich ist.

Das Handbuch dient folgenden Zwecken:

- Hilfe bei der Installation, Aktivierung und Verwendung von Kaspersky Internet Security.
- Schnelle Beantwortung von Fragen, die sich auf die Arbeit des Programms beziehen.
- Hinweise auf zusätzliche Informationsquellen zum Programm und auf Möglichkeiten des technischen Supports.

Um das Programm zu bedienen, sollten Sie über folgende Grundkenntnisse im Umgang mit einem Computer verfügen: Kenntnis der Benutzeroberfläche und der grundlegenden Funktionen des verwendeten Betriebssystems, Arbeit mit E-Mails und Internet.

IN DIESEM ABSCHNITT

IN DIESEM HANDBUCH

Dieses Handbuch enthält folgende Abschnitte:

Informationsquellen zum Programm

Dieser Abschnitt beschreibt Informationsquellen zum Programm und verweist auf Webseiten, die zur Diskussion über das Programm dienen.

Kaspersky Internet Security

Dieser Abschnitt beschreibt die Programm-Features und bietet kurze Informationen zu den Programmfunktionen und -komponenten. Hier werden der Lieferumfang und die Services beschrieben, die den registrierten Programmnutzern zur Verfügung stehen. Dieser Abschnitt informiert über die Hard- und Softwarevoraussetzungen, die ein Computer erfüllen muss, damit Kaspersky Internet Security installiert werden kann.

Programm installieren und deinstallieren

Dieser Abschnitt informiert über die Installation und Deinstallation des Programms.

Lizenzierung des Programms

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmaktivierung zusammenhängen. Hier werden Lizenzvertrag, Lizenztypen, Methoden zur Programmaktivierung und Verlängerung der Lizenzgültigkeit erläutert.

Programmoberfläche

Dieser Abschnitt informiert über die wichtigsten Elemente der grafischen Programmoberfläche: Programmsymbol und Kontextmenü des Programmsymbols, Hauptfenster, Konfigurationsfenster und Meldungsfenster.

Programm starten und beenden

Dieser Abschnitt informiert darüber, wie das Programm gestartet und beendet wird.

Computerschutz verwalten

Dieser Abschnitt informiert darüber, wie Bedrohungen für die Computersicherheit erkannt werden und wie die Sicherheitsstufe angepasst wird. Hier finden Sie außerdem Informationen darüber, wie der Schutz während der Arbeit des Programms aktiviert, deaktiviert oder vorübergehend angehalten werden kann.

Lösungen für typische Aufgaben

Dieser Abschnitt informiert darüber, wie mit diesem Programm grundlegende Aufgaben für den Computerschutz gelöst werden.

Erweiterte Programmeinstellungen

Dieser Abschnitt informiert darüber, wie die einzelnen Programmkomponenten angepasst werden.

Überprüfung der Programmfunktion

Dieser Abschnitt beschreibt, wie die Programmfunktion überprüft und sichergestellt wird, ob das Programm Viren und deren Modifikationen korrekt erkennt und entsprechend behandelt.

Kontaktaufnahme mit dem Technischen Support

Dieser Abschnitt beschreibt die Kontaktaufnahme mit dem Technischen Support.

Anhänge

Dieser Abschnitt enthält Informationen, die den Haupttext des Dokuments ergänzen.

Glossar

Dieser Abschnitt enthält eine Liste und Definitionen von Begriffen, die in diesem Dokument vorkommen.

Kaspersky Lab ZAO

Dieser Abschnitt enthält Informationen über ZAO Kaspersky Lab.

Informationen über den Code von Drittherstellern

Dieser Abschnitt enthält Informationen über den Code von Drittherstellern, der im Programm verwendet wird.

Sachregister

Dieser Abschnitt ermöglicht das schnelle Auffinden bestimmter Angaben in diesem Dokument.

FORMATIERUNG MIT BESONDERER BEDEUTUNG

Das Dokument enthält Textelemente (Warnungen, Tipps, Beispiele), die besondere Beachtung verdienen.

Zur Hervorhebung solcher Elemente werden spezielle Formatierungen verwendet. Ihre Bedeutung wird mit Beispielen in folgender Tabelle erläutert.

Tabelle 1. Formatierung mit besonderer Bedeutung

TEXTBEISPIEL	BESCHREIBUNG DER FORMATIERUNG
Beachten Sie, dass ...	Warnungen sind rot hervorgehoben und eingerahmt. Warnungen informieren darüber, dass unerwünschte Aktionen möglich sind, die zu Datenverlust oder zur Infektion des Computers führen können.
Es wird empfohlen,...	Hinweise sind eingerahmt. Hinweise können nützliche Tipps, Empfehlungen und spezielle Werte enthalten oder sich auf wichtige Sonderfälle bei der Arbeit mit dem Programm beziehen.
Beispiel: ...	Beispiele befinden sich in gelb unterlegten Blöcken und sind mit "Beispiel" überschrieben.
Das *Update* ist... Das Ereignis *Die Datenbanken sind veraltet* tritt ein.	Folgende Textelemente sind kursiv geschrieben. • neue Begriffe • Namen von Statusvarianten und Programmereignissen
Drücken Sie die Taste **ENTER**. Drücken Sie die Tastenkombination **ALT+F4**.	Bezeichnungen von Tasten sind halbfett und in Großbuchstaben geschrieben. Tastenbezeichnungen, die durch ein Pluszeichen verbunden sind, bedeuten eine Tastenkombination. Die genannten Tasten müssen gleichzeitig gedrückt werden.
Klicken Sie auf **Aktivieren**.	Die Namen von Elementen der Programmoberfläche sind halbfett geschrieben (z.B. Eingabefelder, Menüpunkte, Schaltflächen).
➡ *Gehen Sie folgendermaßen vor, um den Aufgabenzeitplan anzupassen:*	Der erste Satz einer Anleitung ist kursiv geschrieben und wird durch einen Pfeil markiert.
Geben Sie in der Befehlszeile den Text `help` ein. Es erscheint folgende Meldung: `Geben Sie das Datum im Format TT:MM:JJ an.`	Folgende Textarten werden durch eine spezielle Schriftart hervorgehoben: • Text einer Befehlszeile • Text von Nachrichten, die das Programm auf dem Bildschirm anzeigt. • Daten, die vom Benutzer eingegeben werden müssen.
`<IP-Adresse Ihres Computers>`	Variablen stehen in eckigen Klammern. Eine Variable muss durch einen entsprechenden Wert ersetzt werden. Dabei fallen die eckigen Klammern weg.

INFORMATIONSQUELLEN ZUM PROGRAMM

Dieser Abschnitt beschreibt Informationsquellen zum Programm und verweist auf Webseiten, die zur Diskussion über das Programm dienen.

Sie können abhängig von der Dringlichkeit und Bedeutung Ihrer Frage eine passende Quelle wählen.

IN DIESEM ABSCHNITT

INFORMATIONSQUELLEN ZUR SELBSTÄNDIGEN RECHERCHE

Sie können folgende Quellen verwenden, um nach Informationen zum Programm zu suchen:

- Seite auf der Webseite von Kaspersky Lab
- Seite auf der Webseite des Technischen Supports (Wissensdatenbank)
- elektronisches Hilfesystem
- Dokumentation

Wenn Sie keine Lösung für Ihr Problem finden können, wenden Sie sich an den Technischen Support von Kaspersky Lab (s. Abschnitt "Technischer Support am Telefon" auf S. 193).

Um die Informationsquellen auf der Kaspersky-Lab-Webseite zu nutzen, ist eine Internetverbindung erforderlich.

Seite auf der Webseite von Kaspersky Lab

Die Kaspersky-Lab-Webseite bietet für jedes Programm eine spezielle Seite.

Auf der Seite (http://www.kaspersky.de/kaspersky_internet_security) finden Sie allgemeine Informationen über das Programm, seine Funktionen und Besonderheiten.

Auf der Seite http://www.kaspersky.de befindet sich ein Link zum Online-Shop. Dort können Sie ein Programm kaufen oder die Nutzungsrechte für das Programm verlängern.

Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

Die Wissensdatenbank auf der Webseite des Technischen Supports (http://support.kaspersky.com/de/desktop) enthält Tipps zur Arbeit mit Kaspersky-Lab-Programmen. Die Wissensdatenbank bietet Hilfeartikel, die nach Themen angeordnet sind.

Auf der Seite des Programms finden Sie in der Wissensdatenbank (http://support.kaspersky.de/kis2012) nützliche Informationen, Tipps und Antworten auf häufige Fragen. Dabei werden Fragen wie Kauf, Installation und Verwendung des Programms behandelt.

Neben Fragen zu Kaspersky Internet Security können die Artikel auch andere Kaspersky-Lab-Programme betreffen und Neuigkeiten über den Technischen Support enthalten.

Elektronisches Hilfesystem

Das elektronische Hilfesystem des Programms umfasst verschiedene Hilfedateien.

Die Kontexthilfe bietet Informationen über die einzelnen Programmfenster: Liste und Beschreibung der Einstellungen und Liste der entsprechenden Aufgaben.

Die vollständige Hilfe enthält ausführliche Informationen darüber, wie der Computerschutz mit diesem Programm verwaltet wird.

Dokumentation

Das Benutzerhandbuch des Programms enthält Informationen zur Installation, Aktivierung und Konfiguration des Programms sowie zur Arbeit mit dem Programm. Das Handbuch bietet eine Beschreibung der Programmoberfläche und Lösungswege für typische Aufgaben, die sich dem Anwender bei der Arbeit mit dem Programm stellen.

DISKUSSION ÜBER DIE PROGRAMME VON KASPERSKY LAB IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum (http://forum.kaspersky.com) diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Beiträge schreiben und neue Themen zur Diskussion stellen.

KONTAKTAUFNAHME MIT DER VERTRIEBSABTEILUNG

Bei Fragen zur Auswahl oder zum Kauf des Programms sowie zur Verlängerung der Nutzungsdauer stehen Ihnen die Mitarbeiter der Vertriebsabteilung zur Verfügung (http://www.kaspersky.de/kontakt).

PER E-MAIL KONTAKT MIT DER ABTEILUNG FÜR HANDBÜCHER UND HILFESYSTEME AUFNEHMEN

Die Abteilung für Handbücher und Hilfesysteme ist per E-Mail zu erreichen. Sie erreichen uns unter docfeedback@kaspersky.de, bitte geben Sie folgenden Betreff an: "Kaspersky Help Feedback: Kaspersky Internet Security".

KASPERSKY INTERNET SECURITY

Dieser Abschnitt beschreibt die Programm-Features und bietet kurze Informationen zu den Programmfunktionen und -komponenten. Hier werden der Lieferumfang und die Services beschrieben, die den registrierten Programmnutzern zur Verfügung stehen. Dieser Abschnitt informiert über die Hard- und Softwarevoraussetzungen, die ein Computer erfüllen muss, damit Kaspersky Internet Security installiert werden kann.

IN DIESEM ABSCHNITT

NEUERUNGEN

Kaspersky Internet Security verfügt über folgende Neuerungen:

- Die verbesserte Benutzeroberfläche des Hauptfensters von Kaspersky Internet Security gewährleistet schnellen Zugriff auf die Programmfunktionen.
- Die Verwendung der Quarantäne und des Backups (s. S. 169) wurde optimiert: Sie befinden sich jetzt auf separaten Registerkarten und führen unterschiedliche Funktionen aus.
- Für die bequeme Verwaltung der Aufgaben verfügt Kaspersky Internet Security jetzt über die Aufgabenübersicht (s. Abschnitt "Untersuchungsaufgaben verwalten. Aufgabenübersicht" auf S. 76).
- Durch die Teilnahme am Kaspersky Security Network (s. S. 184) können Sie Reputation von Programmen und Webseiten ermitteln. Dazu dienen Daten, die von Benutzern aus der ganzen Welt stammen.
- Bei aktiviertem Web-Anti-Virus lässt sich die heuristische Analyse für die Phishing-Prüfung von Webseiten separat aktivieren (s. Abschnitt "Heuristische Analyse für Web-Anti-Virus verwenden" auf S. 98). Dabei wird die heuristische Analyse bei der Phishing-Prüfung unabhängig davon verwendet, ob die heuristische Analyse für Web-Anti-Virus aktiviert wurde.
- Das Aussehen von Kaspersky Gadget (s. S. 39) wurde verändert.

LIEFERUMFANG

Sie können das Programm folgendermaßen kaufen:

- **In einer Box**. Verkauf über unsere Vertriebspartner.
- **Über den Online-Shop**. Verkauf über den Online-Shop von Kaspersky Lab (beispielsweise http://www.kaspersky.com/de/store) oder unserer Vertriebspartner.

Wenn Sie das Programm in einer CD-Box erworben haben, umfasst der Lieferumfang folgende Elemente:

- versiegelter Umschlag mit Installations-CD, auf der die Programmdateien und die Dateien der Programmdokumentation gespeichert sind.

- Kurzanleitung, die einen Aktivierungscode für das Programm enthält.
- Lizenzvertrag, der die Nutzungsbedingungen für das Programm festlegt.

Der Lieferumfang kann sich je nach Region, in der das Programm vertrieben wird, unterscheiden.

Wenn Sie Kaspersky Internet Security in einem Online-Shop kaufen, kopieren Sie das Programm von der Seite des Online-Shops. Sie erhalten die zur Programmaktivierung erforderlichen Informationen nach Eingang des Rechnungsbetrags per E-Mail.

Ausführliche Informationen zum Kauf und Lieferumfang erhalten Sie bei unserer Vertriebsabteilung.

SERVICE FÜR REGISTRIERTE BENUTZER

Durch den Kauf einer Lizenz für die Programmnutzung werden Sie zum registrierten Benutzer eines Kaspersky-Lab-Programms und können während der Gültigkeitsdauer der Lizenz folgende Leistungen in Anspruch nehmen:

- Update der Datenbanken und Nutzung neuer Programmversionen
- Beratung bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und E-Mail
- Benachrichtigung über das Erscheinen neuer Kaspersky-Lab-Programme und über neue Viren. Diesen Service können Sie nutzen, wenn Sie auf der Webseite des Technischen Supports den Newsletter von Kaspersky Lab abonnieren.

  Die Beratung erstreckt sich nicht auf Fragen über die Funktionsweise von Betriebssystemen, der Software von Drittherstellern und sonstiger Technologien.

HARD- UND SOFTWAREVORAUSSETZUNGEN

Um die normale Funktionsfähigkeit von Kaspersky Anti-Virus zu gewährleisten, sind folgende Systemvoraussetzungen zu erfüllen:

Allgemeine voraussetzungen:

- 480 MB freier Speicherplatz auf der Festplatte (einschl. 380 MB auf dem Systemlaufwerk)
- CD / DVD-ROM-Laufwerk (für Installation von Kaspersky Internet Security von Installations-CD)
- Internetverbindung (für die Aktivierung des Programms und für das Update der Datenbanken und Programm-Module)
- Microsoft Internet Explorer 6.0 oder höher
- Microsoft Windows Installer 2.0

Anforderungen für die Betriebssysteme Microsoft Windows XP Home Edition (Service Pack 2 oder höher), Microsoft Windows XP Professional (Service Pack 2 oder höher), Microsoft Windows XP Professional x64 Edition (Service Pack 2 oder höher):

- Prozessor Intel Pentium 800 MHz 32-Bit (x86) / 64-Bit (x64) oder höher (oder ein kompatibler Prozessor)
- 512 MB freier Arbeitsspeicher.

Anforderungen für die Betriebssysteme Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate:

- Prozessor Intel Pentium 1 GHz 32-Bit (x86) / 64-Bit (x64) oder höher (oder ein kompatibler Prozessor)
- 1 GB freier Arbeitsspeicher für 32-Bit-Betriebssysteme, 2 GB freier Arbeitsspeicher für 64-Bit-Betriebssysteme

Anforderungen für Netbooks:

- Prozessor Intel Atom 1,6 GHz (Z520) oder ein entsprechender kompatibler Prozessor
- Grafikkarte Intel GMA950 mit Videospeicher von mindestens 64 MB (oder kompatibel)
- Bildschirmdiagonale mindestens 10.1 Zoll

PROGRAMM INSTALLIEREN UND DEINSTALLIEREN

Dieser Abschnitt informiert über die Installation und Deinstallation des Programms.

IN DIESEM ABSCHNITT

STANDARD-INSTALLATIONSMETHODE

Kaspersky Internet Security wird auf dem Computer interaktiv mit einem Installationsassistenten installiert.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Wenn das Programm für den Schutz von mehr als einem Computer eingesetzt wird (die maximal zulässige Anzahl der Computer ist von Ihrer Lizenz abhängig), wird es auf allen Computern in der gleichen Weise installiert. Hierbei ist zu beachten, dass die Gültigkeitsdauer der Lizenz gemäß Lizenzvereinbarung mit der ersten Aktivierung des Programms beginnt. Wenn das Programm auf einem zweiten und weiteren Computern installiert wird, verkürzt sich auf diesen die Lizenzgültigkeit um die Zeitspanne, die seit der ersten Aktivierung verstrichen ist. Somit läuft die Lizenz aller installierten Kopien des Programms gleichzeitig ab.

➡ *Zur Installation von Kaspersky Internet Security auf Ihrem Computer,*

starten Sie auf der CD-ROM mit dem Programm die ausführbare Datei (mit der Endung exe).

Der Installationsvorgang für das Programm Kaspersky Internet Security, das aus dem Internet bezogen wurde, ist identisch mit dem Installationsvorgang von der CD-ROM.

IN DIESEM ABSCHNITT

SCHRITT 1. NACH NEUER PROGRAMMVERSION SUCHEN

Vor der Installation wird geprüft, ob neuere Versionen von Kaspersky Internet Security auf den Updateservern von Kaspersky Lab vorhanden sind.

Wenn keine neuere Version des Programms auf den Updateservern von Kaspersky Lab gefunden wurde, wird der Installationsassistent für diese Version gestartet.

Wenn auf den Updateservern eine neuere Version von Kaspersky Internet Security vorgefunden wurde, werden Ihnen Download und Installation vorgeschlagen. Es wird empfohlen, die neue Programmversion zu installieren, da neue Versionen den Schutz Ihres Computers optimieren. Sollten Sie die neuere Version ablehnen, wird der Installationsassistent der laufenden Version gestartet. Sollten Sie die Installation der neueren Version annehmen, werden die Programmdateien auf Ihren Computer kopiert und der Installationsassistent wird automatisch gestartet. Eine weitere Beschreibung zur Installation einer neueren Version finden Sie in der Dokumentation zur entsprechenden Programmversion.

SCHRITT 2. SYSTEMKOMPATIBILITÄT FÜR INSTALLATION PRÜFEN

Vor der Installation von Kaspersky Internet Security auf Ihrem Computer wird die Kompatibilität des Betriebssystems und der Service Packs mit den Softwarevoraussetzungen für die Installation abgeglichen (s. Abschnitt "Hard- und Softwarevoraussetzungen" auf S. 17). Außerdem werden die Hardwarevoraussetzungen sowie die Rechte für die Installation des Programms geprüft. Wenn eine der aufgezählten Bedingungen nicht erfüllt wird, erscheint eine entsprechende Meldung auf dem Bildschirm.

Wenn der Computer die Voraussetzungen erfüllt, sucht der Assistent nach Kaspersky-Lab-Programmen, deren gleichzeitige Verwendung mit Kaspersky Internet Security zu Konflikten führen kann. Wenn solche Programme gefunden werden, werden Sie aufgefordert, die Programme manuell zu entfernen.

Wenn sich unter den gefundenen Programmen eine Vorgängerversion von Kaspersky Anti-Virus oder Kaspersky Internet Security befindet, werden alle Daten, die von Kaspersky Internet Security 2012 verwendet werden können (z.B. Aktivierungsdaten oder Programmeinstellungen), gespeichert und bei der Installation verwendet, und das bereits installierte Programm wird automatisch gelöscht.

SCHRITT 3. INSTALLATIONSTYP WÄHLEN

In dieser Phase der Installation können Sie einen passenden Typ für die Installation von Kaspersky Internet Security auswählen:

- *Standardmäßige Installation*. Bei dieser Variante (das Kontrollkästchen **Installationseinstellungen ändern** ist deaktiviert) wird das Programm in vollem Umfang mit den von Kaspersky-Lab-Fachleuten empfohlenen Schutzeinstellungen auf Ihrem Computer installiert.

- *Installation mit der Möglichkeit zur Parameteränderung*. In diesem Fall (das Kontrollkästchen **Installationseinstellungen ändern** ist aktiviert) werden Sie gebeten, einen Installationsordner für das Programm anzugeben und bei Bedarf den Schutz des Installationsprozesses zu aktivieren (s. Abschnitt "Schritt

7. Installationsverzeichnis wählen" auf S. 21) und bei Bedarf den Schutz des Installationsprozesses aktivieren (s. Abschnitt "Schritt 8. Installation vorbereiten" auf S. 22).

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 4. LIZENZVEREINBARUNG ANZEIGEN

In dieser Phase müssen Sie die Lizenzvereinbarung lesen, die zwischen Ihnen und Kaspersky Lab eingegangen wird.

Lesen Sie sich die Vereinbarung sorgfältig durch und wenn Sie mit allen Punkten einverstanden sind, klicken Sie auf die Schaltfläche **Akzeptieren**. Die Installation des Programms auf Ihrem Computer wird fortgesetzt.

Wenn Sie der Lizenzvereinbarung nicht zustimmen, brechen Sie die Programminstallation durch Klick auf **Abbrechen** ab.

SCHRITT 5. ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

Bei diesem Schritt wird Ihnen angeboten, an dem Programm Kaspersky Security Network teilzunehmen. Eine Beteiligung an diesem Programm sieht vor, dass Informationen über auf Ihrem Computer erkannte neue Bedrohungen, über gestartete Programme und über geladene signierte Programme, sowie Systeminformationen an Kaspersky Lab geschickt werden. Es wird dabei garantiert, dass keine persönlichen Daten gesendet werden.

Lesen Sie sich die Erklärung zur Verwendung von Kaspersky Security Network gründlich durch. Um den gesamten Text der Vereinbarung aufzurufen, klicken Sie bitte auf die Schaltfläche **Vollständige KSN-Vereinbarung**. Wenn Sie mit allen Punkten einverstanden sind, setzen Sie im Assistentenfenster das Häkchen im Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen des Kaspersky Security Network**.

Klicken Sie auf **Weiter**, wenn Sie die Installation mit der Möglichkeit zur Konfigurationsänderung ausführen (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 20). Klicken Sie im Fall einer standardmäßigen Installation auf **Installieren**. Die Installation wird fortgesetzt.

SCHRITT 6. INKOMPATIBLE PROGRAMME SUCHEN

In dieser Phase wird geprüft, ob auf Ihrem Computer Programme installiert sind, die nicht mit Kaspersky Internet Security kompatibel sind.

Wenn keine derartigen Programme gefunden werden, geht der Assistent automatisch zum nächsten Schritt.

Werden inkompatible Programme gefunden, so wird eine entsprechende Liste auf dem Bildschirm angezeigt und Sie werden aufgefordert, die Programme zu entfernen. Programme, die von Kaspersky Internet Security nicht automatisch entfernt werden können, müssen manuell deinstalliert werden. Im Verlauf der Deinstallation inkompatibler Programme wird das System neu gestartet. Anschließend wird die Installation von Kaspersky Internet Security automatisch fortgesetzt.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 7. INSTALLATIONSVERZEICHNIS WÄHLEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn die Programminstallation mit der Möglichkeit zur Konfigurationsänderung erfolgt (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 20). Bei der standardmäßigen Installation wird dieser Schritt übersprungen und das Programm wird in dem standardmäßig hierfür vorgesehenen Ordner installiert.

In dieser Phase der Installation wird Ihnen vorgeschlagen, den Ordner zu bestimmen, in den Kaspersky Internet Security installiert wird. Standardmäßig gilt folgender Pfad:

- **<Datenträger>\Programme\Kaspersky Lab\Kaspersky Internet Security 2012** – für 32-Bit-Systeme.
- **<Datenträger>\Programme(x86)\Kaspersky Lab\Kaspersky Internet Security 2012** – für 64-Bit-Systeme.

Um Kaspersky Internet Security in einem anderen Ordner zu installieren, geben Sie bitte den entsprechenden Pfad im Eingabefeld an oder klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie in dem erscheinenden Fenster den gewünschten Ordner aus.

Bitte beachten Sie die folgenden Einschränkungen:

- Das Programm darf weder auf Netzlaufwerken oder Wechseldatenträgern noch auf virtuellen Laufwerken, die mit dem Befehl `SUBST` erstellt wurden, installiert werden.
- Es wird davor gewarnt, das Programm in einem Ordner zu installieren, der bereits Dateien oder andere Ordner enthält, da der Zugriff auf den Ordner anschließend verboten werden kann.
- Der Pfad des Installationsordners darf höchstens 160 Zeichen lang sein und keines der Sonderzeichen **/**, **?**, **:**, *****, **"**, **>**, **<** und **|** enthalten.

Um festzustellen, ob auf Ihrem Computer ausreichend Speicherplatz für die Installation der Anwendung vorhanden ist, klicken Sie auf die Schaltfläche **Laufwerk**. Das daraufhin erscheinende Fenster enthält Informationen zum verfügbaren Speicherplatz. Um das Fenster zu schließen, klicken Sie auf **OK**.

Zum Fortsetzen der Installation klicken Sie im Fenster des Assistenten auf die Schaltfläche **Weiter**.

SCHRITT 8. INSTALLATION VORBEREITEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn die Programminstallation mit der Möglichkeit zur Konfigurationsänderung erfolgt (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 20). Bei der standardmäßigen Installation wird dieser Schritt übersprungen.

Da sich auf Ihrem Computer schädliche Programme befinden können, die fähig sind, die Installation von Kaspersky Internet Security zu stören, muss der Installationsprozess geschützt werden.

Der Schutz des Installationsprozesses ist standardmäßig aktiviert – im Fenster des Assistenten ist das Kontrollkästchen **Installationsprozess schützen** angekreuzt.

Es wird empfohlen, das Kontrollkästchen zu deaktivieren, wenn die Programminstallation andernfalls nicht möglich ist (dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein). Der Grund kann im aktivierten Schutz liegen.

Brechen Sie in diesem Fall die Installation ab und starten Sie den Installationsprozess erneut. Aktivieren Sie beim Schritt Installationstyp wählen das Kontrollkästchen **Installationseinstellungen ändern** (s. Abschnitt "Schritt 3. Installationstyp wählen" auf S. 20) und deaktivieren Sie beim Schritt zur Installationsvorbereitung das Kontrollkästchen **Installationsprozess schützen**.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Installieren**.

Bei der Installation des Programms auf einem Computer mit dem Betriebssystem Microsoft Windows XP werden bestehende Netzwerkverbindungen getrennt. Die Mehrzahl der getrennten Verbindungen wird nach einiger Zeit wiederhergestellt.

SCHRITT 9. INSTALLATION

Die Installation des Programms nimmt einige Zeit in Anspruch. Warten Sie die Fertigstellung ab.

Der Assistent geht nach Abschluss der Installation automatisch zum nächsten Schritt.

Falls bei der Installation ein Fehler auftritt, der möglicherweise durch auf dem Computer vorhandene Schadprogramme verursacht wurde, die eine Installation von Antiviren-Programmen verhindern, schlägt der Installationsassistent vor, das spezielle Hilfsprogramm *Kaspersky Virus Removal Tool* herunterzuladen, um die Infektion zu beseitigen.

Wenn Sie der Installation des Tools zustimmen, lädt der Installationsassistent es von den Kaspersky-Lab-Servern herunter und startet anschließend automatisch die Installation des Tools. Gelingt dem Assistenten der Download des Tools nicht, so werden Sie aufgefordert, es über einen Link manuell herunterzuladen.

Nachdem das Tool seine Arbeit abgeschlossen hat, muss es entfernt werden. Anschließend wird die Installation von Kaspersky Internet Security erneut gestartet.

SCHRITT 10. INSTALLATION ABSCHLIEßEN

Dieses Fenster des Assistenten informiert über den Abschluss der Programminstallation. Um mit der Arbeit von Kaspersky Internet Security zu beginnen, vergewissern Sie sich, dass das Kontrollkästchen **Kaspersky Internet Security 2012 starten** aktiviert ist und klicken Sie auf **Beenden**.

In einigen Fällen kann ein Neustart des Betriebssystems erforderlich sein. Wenn das Kontrollkästchen **Kaspersky Internet Security 2012 starten** aktiviert ist, wird das Programm nach einem Reboot automatisch gestartet.

Wenn Sie das Kontrollkästchen vor dem Abschluss des Assistenten deaktiviert haben, muss das Programm manuell gestartet werden (s. Abschnitt "Programm manuell starten und beenden" auf S. 41).

SCHRITT 11. PROGRAMM AKTIVIEREN

Durch die *Aktivierung* erlangt die Lizenz für die Nutzung der Vollversion des Programms ihre Gültigkeit für den entsprechenden Zeitraum.

Um das Programm zu aktivieren, ist eine Internetverbindung erforderlich.

Für die Aktivierung von Kaspersky Internet Security bestehen folgende Möglichkeiten:

- **Kommerzielle Version aktivieren**. Wählen Sie diese Option und geben Sie den Aktivierungscode ein, wenn Sie eine kommerzielle Programmversion erworben haben.

  Wenn Sie einen Aktivierungscode für Kaspersky Anti-Virus eingeben, wird nach der Aktivierung eine Umstellung zu Kaspersky Anti-Virus gestartet.

- **Testversion aktivieren**. Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Für die Gültigkeitsdauer der Lizenz für die Testversion können Sie das Programm mit uneingeschränktem Funktionsumfang verwenden. Nach Ablauf der Lizenz ist es nicht möglich, erneut eine Testlizenz zu aktivieren.

SCHRITT 12. ANMELDUNG DES BENUTZERS

Dieser Schritt ist nur bei der Aktivierung einer kommerziellen Programmversion verfügbar. Bei der Aktivierung einer Testversion wird der Schritt übersprungen.

Um auch weiterhin die Möglichkeit zu haben, den Technischen Support von Kaspersky Lab zu kontaktieren, müssen Sie sich registrieren.

Wenn Sie mit der Anmeldung einverstanden sind, füllen Sie die entsprechenden Felder aus und klicken Sie dann auf **Weiter**, um Ihre Anmeldung abzuschicken.

SCHRITT 13. AKTIVIERUNG ABSCHLIEßEN

Der Assistent informiert Sie über den erfolgreichen Abschluss der Aktivierung von Kaspersky Internet Security. Außerdem werden Informationen über die Lizenz angezeigt: Typ (kommerziell oder Test), Gültigkeitsdauer der Lizenz, sowie Anzahl der Computer, für die die Lizenz gültig ist.

Bei der Aktivierung eines Abonnements werden anstelle des Ablaufdatums für die Lizenz Informationen zum Abo-Status angezeigt.

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

AKTUALISIERUNG EINER VORGÄNGERVERSION VON KASPERSKY INTERNET SECURITY

Wenn Kaspersky Internet Security 2010 oder 2011 bereits auf Ihrem Computer installiert ist, müssen Sie das Programm auf die Version Kaspersky Internet Security 2012 aktualisieren. Bei Vorhandensein einer gültigen Lizenz für Kaspersky Internet Security 2010 oder 2011 müssen Sie das Programm nicht neu aktivieren: Der Installationsassistent erhält automatisch die Informationen über die Lizenz für Kaspersky Internet Security 2010 oder 2011 und verwendet diese beim Installationsvorgang.

Kaspersky Internet Security wird auf dem Computer interaktiv mit einem Installationsassistenten installiert.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Wenn das Programm für den Schutz von mehr als einem Computer eingesetzt wird (die maximal zulässige Anzahl der Computer ist von Ihrer Lizenz abhängig), wird es auf allen Computern in der gleichen Weise installiert. Hierbei ist zu beachten, dass die Gültigkeitsdauer der Lizenz gemäß Lizenzvereinbarung mit der ersten Aktivierung des Programms beginnt. Wenn das Programm auf einem zweiten und weiteren Computern installiert wird, verkürzt sich auf diesen die Lizenzgültigkeit um die Zeitspanne, die seit der ersten Aktivierung verstrichen ist. Somit läuft die Lizenz aller installierten Kopien des Programms gleichzeitig ab.

➡ *Zur Installation von Kaspersky Internet Security auf Ihrem Computer,*

starten Sie auf der CD-ROM mit dem Programm die ausführbare Datei (mit der Endung exe).

Der Installationsvorgang für das Programm Kaspersky Internet Security, das aus dem Internet bezogen wurde, ist identisch mit dem Installationsvorgang von der CD-ROM.

IN DIESEM ABSCHNITT

SCHRITT 1. NACH NEUER PROGRAMMVERSION SUCHEN

Vor der Installation wird geprüft, ob neuere Versionen von Kaspersky Internet Security auf den Updateservern von Kaspersky Lab vorhanden sind.

Wenn keine neuere Version des Programms auf den Updateservern von Kaspersky Lab gefunden wurde, wird der Installationsassistent für diese Version gestartet.

Wenn auf den Updateservern eine neuere Version von Kaspersky Internet Security vorgefunden wurde, werden Ihnen Download und Installation vorgeschlagen. Es wird empfohlen, die neue Programmversion zu installieren, da neue Versionen den Schutz Ihres Computers optimieren. Sollten Sie die neuere Version ablehnen, wird der Installationsassistent der laufenden Version gestartet. Sollten Sie die Installation der neueren Version annehmen, werden die Programmdateien auf Ihren Computer kopiert und der Installationsassistent wird automatisch gestartet. Eine weitere Beschreibung zur Installation einer neueren Version finden Sie in der Dokumentation zur entsprechenden Programmversion.

SCHRITT 2. SYSTEMKOMPATIBILITÄT FÜR INSTALLATION PRÜFEN

Vor der Installation von Kaspersky Internet Security auf Ihrem Computer wird die Kompatibilität des Betriebssystems und der Service Packs mit den Softwarevoraussetzungen für die Installation abgeglichen (s. Abschnitt "Hard- und Softwarevoraussetzungen" auf S. 17). Außerdem werden die Hardwarevoraussetzungen sowie die Rechte für die Installation des Programms geprüft. Wenn eine der aufgezählten Bedingungen nicht erfüllt wird, erscheint eine entsprechende Meldung auf dem Bildschirm.

Wenn der Computer die Voraussetzungen erfüllt, sucht der Assistent nach Kaspersky-Lab-Programmen, deren gleichzeitige Verwendung mit Kaspersky Internet Security zu Konflikten führen kann. Wenn solche Programme gefunden werden, werden Sie aufgefordert, die Programme manuell zu entfernen.

Wenn sich unter den gefundenen Programmen eine Vorgängerversion von Kaspersky Anti-Virus oder Kaspersky Internet Security befindet, werden alle Daten, die von Kaspersky Internet Security 2012 verwendet werden können (z.B. Aktivierungsdaten oder Programmeinstellungen), gespeichert und bei der Installation verwendet, und das bereits installierte Programm wird automatisch gelöscht.

SCHRITT 3. INSTALLATIONSTYP WÄHLEN

In dieser Phase der Installation können Sie einen passenden Typ für die Installation von Kaspersky Internet Security auswählen:

- *Standardmäßige Installation*. Bei dieser Variante (das Kontrollkästchen **Installationseinstellungen ändern** ist deaktiviert) wird das Programm in vollem Umfang mit den von Kaspersky-Lab-Fachleuten empfohlenen Schutzeinstellungen auf Ihrem Computer installiert.
- *Installation mit der Möglichkeit zur Parameteränderung*. In diesem Fall (das Kontrollkästchen **Installationseinstellungen ändern** ist aktiviert) werden Sie gebeten, einen Installationsordner für das Programm anzugeben und bei Bedarf den Schutz des Installationsprozesses zu aktivieren (s. Abschnitt "Schritt 7. Installationsverzeichnis wählen" auf S. 21) und bei Bedarf den Schutz des Installationsprozesses aktivieren (s. Abschnitt "Schritt 8. Installation vorbereiten" auf S. 22).

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 4. LIZENZVEREINBARUNG ANZEIGEN

In dieser Phase müssen Sie die Lizenzvereinbarung lesen, die zwischen Ihnen und Kaspersky Lab eingegangen wird.

Lesen Sie sich die Vereinbarung sorgfältig durch und wenn Sie mit allen Punkten einverstanden sind, klicken Sie auf die Schaltfläche **Akzeptieren**. Die Installation des Programms auf Ihrem Computer wird fortgesetzt.

Wenn Sie der Lizenzvereinbarung nicht zustimmen, brechen Sie die Programminstallation durch Klick auf **Abbrechen** ab.

SCHRITT 5. ERKLÄRUNG ZUR VERWENDUNG VON KASPERSKY SECURITY NETWORK

Bei diesem Schritt wird Ihnen angeboten, an dem Programm Kaspersky Security Network teilzunehmen. Eine Beteiligung an diesem Programm sieht vor, dass Informationen über auf Ihrem Computer erkannte neue Bedrohungen, über gestartete Programme und über geladene signierte Programme, sowie Systeminformationen an Kaspersky Lab geschickt werden. Es wird dabei garantiert, dass keine persönlichen Daten gesendet werden.

Lesen Sie sich die Erklärung zur Verwendung von Kaspersky Security Network gründlich durch. Um den gesamten Text der Vereinbarung aufzurufen, klicken Sie bitte auf die Schaltfläche **Vollständige KSN-Vereinbarung**. Wenn Sie mit allen Punkten einverstanden sind, setzen Sie im Assistentenfenster das Häkchen im Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen des Kaspersky Security Network**.

Klicken Sie auf **Weiter**, wenn Sie die Installation mit der Möglichkeit zur Konfigurationsänderung ausführen (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 20). Klicken Sie im Fall einer standardmäßigen Installation auf **Installieren**. Die Installation wird fortgesetzt.

SCHRITT 6. INKOMPATIBLE PROGRAMME SUCHEN

In dieser Phase wird geprüft, ob auf Ihrem Computer Programme installiert sind, die nicht mit Kaspersky Internet Security kompatibel sind.

Wenn keine derartigen Programme gefunden werden, geht der Assistent automatisch zum nächsten Schritt.

Werden inkompatible Programme gefunden, so wird eine entsprechende Liste auf dem Bildschirm angezeigt und Sie werden aufgefordert, die Programme zu entfernen. Programme, die von Kaspersky Internet Security nicht automatisch entfernt werden können, müssen manuell deinstalliert werden. Im Verlauf der Deinstallation inkompatibler Programme wird das System neu gestartet. Anschließend wird die Installation von Kaspersky Internet Security automatisch fortgesetzt.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Weiter**.

SCHRITT 7. INSTALLATIONSVERZEICHNIS WÄHLEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn die Programminstallation mit der Möglichkeit zur Konfigurationsänderung erfolgt (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 20). Bei der standardmäßigen Installation wird dieser Schritt übersprungen und das Programm wird in dem standardmäßig hierfür vorgesehenen Ordner installiert.

In dieser Phase der Installation wird Ihnen vorgeschlagen, den Ordner zu bestimmen, in den Kaspersky Internet Security installiert wird. Standardmäßig gilt folgender Pfad:

- **<Datenträger>\Programme\Kaspersky Lab\Kaspersky Internet Security 2012** – für 32-Bit-Systeme.
- **<Datenträger>\Programme(x86)\Kaspersky Lab\Kaspersky Internet Security 2012** – für 64-Bit-Systeme.

Um Kaspersky Internet Security in einem anderen Ordner zu installieren, geben Sie bitte den entsprechenden Pfad im Eingabefeld an oder klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie in dem erscheinenden Fenster den gewünschten Ordner aus.

Bitte beachten Sie die folgenden Einschränkungen:

- Das Programm darf weder auf Netzlaufwerken oder Wechseldatenträgern noch auf virtuellen Laufwerken, die mit dem Befehl `SUBST` erstellt wurden, installiert werden.
- Es wird davor gewarnt, das Programm in einem Ordner zu installieren, der bereits Dateien oder andere Ordner enthält, da der Zugriff auf den Ordner anschließend verboten werden kann.
- Der Pfad des Installationsordners darf höchstens 160 Zeichen lang sein und keines der Sonderzeichen **/**, **?**, **:**, *****, **"**, **>**, **<** und **|** enthalten.

Um festzustellen, ob auf Ihrem Computer ausreichend Speicherplatz für die Installation der Anwendung vorhanden ist, klicken Sie auf die Schaltfläche **Laufwerk**. Das daraufhin erscheinende Fenster enthält Informationen zum verfügbaren Speicherplatz. Um das Fenster zu schließen, klicken Sie auf **OK**.

Zum Fortsetzen der Installation klicken Sie im Fenster des Assistenten auf die Schaltfläche **Weiter**.

SCHRITT 8. INSTALLATION VORBEREITEN

Dieser Schritt des Installationsassistenten ist nur dann verfügbar, wenn die Programminstallation mit der Möglichkeit zur Konfigurationsänderung erfolgt (s. Abschnitt "Schritt 3. Installationstyp auswählen" auf S. 20). Bei der standardmäßigen Installation wird dieser Schritt übersprungen.

Da sich auf Ihrem Computer schädliche Programme befinden können, die fähig sind, die Installation von Kaspersky Internet Security zu stören, muss der Installationsprozess geschützt werden.

Der Schutz des Installationsprozesses ist standardmäßig aktiviert – im Fenster des Assistenten ist das Kontrollkästchen **Installationsprozess schützen** angekreuzt.

Es wird empfohlen, das Kontrollkästchen zu deaktivieren, wenn die Programminstallation andernfalls nicht möglich ist (dies kann beispielsweise bei einer Remote-Installation über Windows Remote Desktop der Fall sein). Der Grund kann im aktivierten Schutz liegen.

Brechen Sie in diesem Fall die Installation ab und starten Sie den Installationsprozess erneut. Aktivieren Sie beim Schritt Installationstyp wählen das Kontrollkästchen **Installationseinstellungen ändern** (s. Abschnitt "Schritt 3. Installationstyp wählen" auf S. 20) und deaktivieren Sie beim Schritt zur Installationsvorbereitung das Kontrollkästchen **Installationsprozess schützen**.

Zum Fortsetzen der Installation klicken Sie auf die Schaltfläche **Installieren**.

Bei der Installation des Programms auf einem Computer mit dem Betriebssystem Microsoft Windows XP werden bestehende Netzwerkverbindungen getrennt. Die Mehrzahl der getrennten Verbindungen wird nach einiger Zeit wiederhergestellt.

SCHRITT 9. INSTALLATION

Die Installation des Programms nimmt einige Zeit in Anspruch. Warten Sie die Fertigstellung ab.

Der Assistent geht nach Abschluss der Installation automatisch zum nächsten Schritt.

Falls bei der Installation ein Fehler auftritt, der möglicherweise durch auf dem Computer vorhandene Schadprogramme verursacht wurde, die eine Installation von Antiviren-Programmen verhindern, schlägt der Installationsassistent vor, das Hilfsprogramm *Kaspersky Virus Removal Tool* herunterzuladen, um die Infektion zu beseitigen.

Wenn Sie der Installation des Tools zustimmen, lädt der Installationsassistent es von den Kaspersky-Lab-Servern herunter und startet anschließend automatisch die Installation des Tools. Gelingt dem Assistenten der Download des Tools nicht, so werden Sie aufgefordert, es über einen Link manuell herunterzuladen.

Nachdem das Tool seine Arbeit abgeschlossen hat, muss es entfernt werden. Anschließend wird die Installation von Kaspersky Internet Security erneut gestartet.

SCHRITT 10. ASSISTENT ABSCHLIEßEN

Dieses Fenster des Assistenten informiert über den Abschluss der Programminstallation. Um mit der Arbeit von Kaspersky Internet Security zu beginnen, vergewissern Sie sich, dass das Kontrollkästchen **Kaspersky Internet Security 2012 starten** aktiviert ist und klicken Sie auf **Beenden**.

In einigen Fällen kann ein Neustart des Betriebssystems erforderlich sein. Wenn das Kontrollkästchen **Kaspersky Internet Security 2012 starten** aktiviert ist, wird das Programm nach einem Reboot automatisch gestartet.

Wenn Sie das Kontrollkästchen vor dem Abschluss des Assistenten deaktiviert haben, muss das Programm manuell gestartet werden (s. Abschnitt "Programm manuell starten und beenden" auf S. 41).

UNTYPISCHE INSTALLATIONSSZENARIEN

In diesem Abschnitt sind Szenarien für die Programminstallation beschrieben, die von der Standard-Installation oder vom Update auf Basis der Vorgängerversion abweichen.

Installation von Kaspersky Internet Security mit anschließender Aktivierung mittels Aktivierungscode von Kaspersky Anti-Virus

Wenn Sie während der Installation von Kaspersky Internet Security bei der Programmaktivierung einen Aktivierungscode für Kaspersky Anti-Virus eingeben, startet ein Vorgang, bei dem Kaspersky Anti-Virus auf Ihrem Computer installiert wird.

Wenn Sie während der Installation von Kaspersky Internet Security bei der Programmaktivierung die Option **Später aktivieren** wählen, und das installierte Programm dann mit einem Aktivierungscode für Kaspersky Anti-Virus aktivieren, startet ebenfalls ein Vorgang, bei dem Kaspersky Anti-Virus auf Ihrem Computer installiert wird.

Installation von Kaspersky Internet Security 2012 über Kaspersky Anti-Virus 2010 oder 2011

Wenn Sie die Installation von Kaspersky Internet Security 2012 auf einem Computer starten, auf dem bereits Kaspersky Anti-Virus 2010 oder 2011 mit einer gültigen Lizenz installiert ist, schlägt Ihnen der Installationsassistent nach Erkennung der Lizenz folgende Optionen für das weitere Vorgehen vor:

- Verwendung der gültigen Lizenz von Kaspersky Anti-Virus 2010 oder 2011. In diesem Fall wird ein Vorgang gestartet, bei dem Kaspersky Anti-Virus 2012 auf Ihrem Computer installiert wird. Sie können Kaspersky Anti-Virus 2012 für die gesamte Lizenzlaufzeit von Kaspersky Anti-Virus 2010 oder 2011 verwenden.
- Fortsetzen der Installation von Kaspersky Internet Security 2012. In diesem Fall wird der Installationsvorgang nach dem Standard-Szenario fortgesetzt und beginnt mit der Programmaktivierung.

ERSTE SCHRITTE

Nach abgeschlossener Installation und Konfiguration ist das Programm einsatzbereit. Um einen effektiven Schutz Ihres Computers zu gewährleisten, empfehlen wir direkt im Anschluss an die Installation und Konfiguration die Durchführung folgender Aktionen:

- Programm-Datenbanken aktualisieren (s. Abschnitt "Datenbanken und Programm-Module aktualisieren" auf S. 48).
- Computer auf Viren untersuchen (s. Abschnitt "Computer vollständig auf Viren untersuchen" auf S. 51) und auf Schwachstellen untersuchen (s. Abschnitt "Computer auf Schwachstellen untersuchen" auf S. 51).
- Schutzstatus des Computers prüfen und bei Bedarf Probleme im Schutz beheben.

PROGRAMM DEINSTALLIEREN

Wenn Kaspersky Internet Security deinstalliert wird, sind der Computer und Ihre persönlichen Daten ungeschützt!

Kaspersky Internet Security wird mit dem Installationsassistenten entfernt.

Um den Assistenten zu starten,

gehen Sie im **Startmenü** auf **Programme** → **Kaspersky Internet Security 2012** → **Kaspersky Internet Security 2012 entfernen**.

IN DIESEM ABSCHNITT

SCHRITT 1. DATEN ZUR ERNEUTEN VERWENDUNG SPEICHERN

Bei diesem Schritt können Sie festlegen, welche vom Programm verwendeten Daten Sie speichern möchten, um sie später bei einer Neuinstallation des Programms (z.B. Installation einer neueren Version) wiederzuverwenden.

In der Grundeinstellung wird das Programm vollständig vom Computer entfernt.

Gehen Sie folgendermaßen vor, um bestimmte Daten zur erneuten Verwendung zu speichern:

1. Wählen Sie die Variante **Objekte der Anwendung speichern**.
2. Aktivieren Sie die Kontrollkästchen der Daten, die gespeichert werden sollen.
   - **Aktivierungsdaten** – Daten, die es erlauben, das zu installierende Programm später nicht zu aktivieren, sondern automatisch die aktive Lizenz zu verwenden, vorausgesetzt, sie zum Zeitpunkt der Installation noch gültig ist.
   - **Backup- und Quarantäneobjekte** – Dateien, die vom Programm untersucht und im Backup und in der Quarantäne gespeichert wurden.
   - **Einstellungen des Programms** – Parameterwerte für die Programmfunktion, die im Verlauf der Programmkonfiguration eingestellt wurden.

- **iChecker-Daten** – Dateien mit Informationen zu den Objekten, die bereits auf Viren untersucht wurden.
- **Daten des gemeinsamen Ordners der Sicheren Umgebung** – Dateien, die bei der Arbeit in der Sicheren Umgebung in einem speziellen Ordner gespeichert wurden, der auch in der normalen Umgebung verfügbar ist.
- **Anti-Spam-Datenbanken** – Datenbanken, die Muster von Spam-Mails enthalten, die das Program bei seiner Arbeit erhalten und gespeichert hat.

SCHRITT 2. PROGRAMMDEINSTALLATION BESTÄTIGEN

Da durch eine Programmdeinstallation der Schutz Ihres Computers und Ihrer persönlichen Daten gefährdet werden kann, muss das Löschen des Programms bestätigt werden. Klicken Sie dazu auf die Schaltfläche **OK**.

Bevor die Deinstallation abgeschlossen wird, können Sie diese Aktion jederzeit durch Klick auf **Abbrechen** verwerfen.

SCHRITT 3. PROGRAMM DEINSTALLIEREN. DEINSTALLATION ABSCHLIEẞEN

Bei diesem Schritt löscht der Assistent das Programm von Ihrem Computer. Warten Sie, bis der Deinstallationsvorgang abgeschlossen wird.

Im Verlauf der Deinstallation kann ein Neustart des Systems erforderlich sein. Wenn Sie einen sofortigen Neustart ablehnen, wird der Abschluss der Deinstallation aufgeschoben, bis das Betriebssystem neu gestartet oder der Computer herunter- und hochgefahren wird.

LIZENZIERUNG DES PROGRAMMS

Dieser Abschnitt informiert über die wichtigsten Begriffe, die mit der Programmaktivierung zusammenhängen. Hier werden Lizenzvertrag, Lizenztypen, Methoden zur Programmaktivierung und Verlängerung der Lizenzgültigkeit erläutert.

IN DIESEM ABSCHNITT

ÜBER DEN LIZENZVERTRAG

Der Lizenzvertrag ist ein rechtsgültiger Vertrag zwischen Ihnen und Kaspersky Lab ZAO. Er bestimmt die Nutzungsbedingungen für das Programm.

Lesen Sie den Lizenzvertrag sorgfältig, bevor Sie beginnen, mit dem Programm zu arbeiten.

Die Bedingungen des Lizenzvertrags können Sie während der Installation des Kaspersky-Lab-Programms einsehen.

Die Bedingungen des Lizenzvertrags gelten in folgenden Fällen als akzeptiert:

- Wenn die Verpackung mit der Installations-CD geöffnet wurde (nur wenn Sie das Programm bei einem Einzelhändler oder in einem unserer Vertriebspartner als Box gekauft haben).
- Wenn Sie bei der Programminstallation den Lizenzvertrag akzeptieren.

Falls Sie dem Lizenzvertrag nicht zustimmen, müssen Sie die Programminstallation abbrechen.

ÜBER DIE ZURVERFÜGUNGSTELLUNG VON DATEN

Wenn Sie die Lizenzvereinbarung akzeptieren, stimmen Sie damit auch zu, dass automatisch folgende Informationen übertragen werden, um das Schutzniveau zu erhöhen: Informationen über die Kontrollsummen verarbeiteter Dateien (MD5), Informationen für die Ermittlung der URL-Reputation, und statistische Daten für den Spam-Schutz. Diese Informationen enthalten keine persönlichen Daten oder vertraulichen Informationen. Diese Informationen werden von Kaspersky Lab in Übereinstimmung mit den gesetzlichen Anforderungen geschützt. Weitere Informationen erhalten Sie auf der Webseite http://support.kaspersky.com.

ÜBER DIE LIZENZ

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für ein Programm, das Ihnen auf Basis eines Lizenzvertrags überlassen wird. Die Lizenz enthält einen individuellen Aktivierungscode für Ihr Exemplar von Kaspersky Internet Security.

Die Lizenz berechtigt Sie zur Nutzung folgender Leistungen:

- Verwendung des Programms auf einem oder mehreren Geräten.

> Die Anzahl der Geräte, auf denen Sie das Programm nutzen dürfen, wird im Lizenzvertrag genannt.

- Kontaktaufnahme mit dem Technischen Support von Kaspersky Lab
- Nutzung des gesamten Leistungspakets, das Ihnen von Kaspersky Lab oder den Vertriebspartnern für die Gültigkeitsdauer der Lizenz angeboten wird (s. Abschnitt "Service für registrierte Benutzer" auf S. 17).

Der Umfang der verfügbaren Leistungen und die Nutzungsdauer für das Programm sind vom Typ der Lizenz abhängig, mit der das Programm aktiviert wurde.

Es sind folgende Lizenztypen vorgesehen

- *Testlizenz* – Kostenlose Lizenz mit begrenzter Gültigkeitsdauer zum Kennenlernen des Programms.

  Wenn Sie das Programm von der Seite http://www.kaspersky.de herunterladen, werden Sie automatisch zum Besitzer einer Testlizenz. Nach Ablauf der Lizenz stellt Kaspersky Internet Security alle Funktionen ein. Es muss eine kommerzielle Lizenz gekauft werden, um das Programm weiter zu verwenden.

- *Kommerziell* – Gekaufte Lizenz mit begrenzter Gültigkeitsdauer. Diese Lizenz erhalten Sie beim Kauf eines Programms.

  Bei Ablauf einer kommerziellen Lizenz arbeitet das Programm im eingeschränkten Modus weiter. Sie können Ihren Computer weiterhin auf Viren untersuchen und die anderen Programmkomponenten verwenden, allerdings nur mit den Datenbanken, die beim Ablauf der Lizenz installiert waren. Die kommerzielle Lizenz muss verlängert werden, um Kaspersky Internet Security weiter zu verwenden.

  Es wird empfohlen, die Gültigkeitsdauer einer Lizenz spätestens dann zu verlängern, wenn die aktive Lizenz abläuft. Nur so lässt sich ein optimaler Antiviren-Schutz für Ihren Computer gewährleisten.

ÜBER DEN AKTIVIERUNGSCODE

Ein *Aktivierungscode* ist ein Code, den Sie beim Kauf einer kommerziellen Lizenz für Kaspersky Internet Security erhalten. Dieser Code ist für die Programmaktivierung erforderlich.

Ein Aktivierungscode besteht aus einer Folge von zwanzig Ziffern und lateinischen Buchstaben im Format xxxxx-xxxxx-xxxxx-xxxxx.

Abhängig davon, auf welche Weise das Programm gekauft wird, wird der Aktivierungscode folgendermaßen geliefert:

- Wenn Sie Kaspersky Internet Security in einer CD-Box gekauft haben, ist der Aktivierungscode in der Dokumentation oder auf der Verpackung angegeben, in der sich die Installations-CD befindet.
- Wenn Sie Kaspersky Internet Security in einem Online-Shop gekauft haben, erhalten Sie den Aktivierungscode per E-Mail an die Adresse, die Sie bei der Bestellung angegeben haben.

Die Gültigkeitsdauer einer Lizenz beginnt mit der Programmaktivierung. Wenn Sie eine Lizenz gekauft haben, die für eine Verwendung von Kaspersky Internet Security auf mehreren Geräten vorgesehen ist, so wird die Gültigkeitsdauer der Lizenz ab der Codeaktivierung auf dem ersten Computer gezählt.

Wenn ein Aktivierungscode verloren oder versehentlich gelöscht wurde, muss eine Anfrage an den Technischen Support von Kaspersky Lab geschickt werden, um den Code wiederherzustellen. Die Anfrage muss über Mein Kaspersky Account erfolgen (s. Abschnitt "Technischen Support erhalten über Mein Kaspersky Account" auf S. 193).

Wenn das Programm mit einem Aktivierungscode aktiviert wird, erhalten Sie eine *Kundennummer*. Eine Kundennummer ist eine individuelle Identifikationsnummer des Benutzers. Sie ist erforderlich, um telefonisch oder in Mein Kaspersky Account technische Unterstützung zu erhalten (s. Abschnitt "Technischen Support erhalten über Mein Kaspersky Account" auf S. 193).

PROGRAMMOBERFLÄCHE

Dieser Abschnitt informiert über die wichtigsten Elemente der grafischen Programmoberfläche: Programmsymbol und Kontextmenü des Programmsymbols, Hauptfenster, Konfigurationsfenster und Meldungsfenster.

IN DIESEM ABSCHNITT

SYMBOL IM INFOBEREICH DER TASKLEISTE

Sofort nach der Installation von Kaspersky Internet Security erscheint sein Symbol im Infobereich der Taskleiste von Microsoft Windows.

Unter dem Betriebssystem Microsoft Windows 7 ist das Programmsymbol standardmäßig ausgeblendet. Es lässt sich wieder einblenden, um mit dem Programm zu arbeiten (s. Dokumentation des Betriebssystems).

Das Symbol besitzt folgende Funktionen:

- Es dient als Indikator für die Arbeit des Programms.
- Es bietet Zugriff auf das Kontextmenü, das Programmhauptfenster und das Nachrichtenfenster.

Indikator für die Programmarbeit

Das Symbol dient als Indikator für die Arbeit des Programms. Es informiert über den Schutzstatus und zeigt eine Reihe wichtiger Aktionen, die vom Programm ausgeführt werden.

– Es wird eine E-Mail-Nachricht untersucht.

– Der Web-Datenverkehr wird untersucht.

– Die Datenbanken und Programm-Module werden aktualisiert.

– Ein Neustart des Computers ist erforderlich, um die Updates zu übernehmen.

– Bei der Arbeit einer Programmkomponente ist eine Störung aufgetreten.

Die Animation des Symbols ist standardmäßig aktiviert: Beispielsweise erscheint bei der Untersuchung einer E-Mail im Hintergrund des Programmsymbols das Piktogramm eines Briefs, beim Update der Programm-Datenbanken

erscheint ein rotierender Globus. Sie können die Animation ausschalten (s. Abschnitt "Halbtransparenz für Meldungsfenster" auf S. 181).

Wenn die Animation aktiviert ist, kann das Symbol folgendes Aussehen annehmen:

(farbiges Symbol) – Alle oder einige Schutzkomponenten sind aktiv.

(schwarz-weißes Symbol) – Alle Schutzkomponenten wurden deaktiviert.

Zugriff auf das Kontextmenü und auf die Programmfenster

Mit Hilfe des Symbols können Sie das Kontextmenü (auf S. 34) (durch Rechtsklick) und das Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 35) (durch Linksklick) öffnen.

Wenn Nachrichten von Kaspersky Lab erschienen sind, wird im Infobereich der Taskleiste von Microsoft Windows das Symbol eingeblendet. Das Fenster für den News Agent (s. Abschnitt "News Agent" auf S. 40) kann durch Doppelklick auf dieses Symbol geöffnet werden.

KONTEXTMENÜ

Über das Kontextmenü können Sie schnell bestimmte Aktionen mit dem Programm ausführen.

Das Menü von Kaspersky Internet Security enthält folgende Punkte:

- **Aufgabenübersicht** – Öffnet das Fenster **Aufgabenübersicht**.
- **Update** – startet die Aktualisierung der Programmdatenbanken und -module.
- **Tools** – Öffnet ein Kontextmenü, das folgende Punkte enthält:
  - **Programmaktivität** – Öffnet das Fenster **Programmaktivität**.
  - **Netzwerkmonitor** – Öffnet das Fenster **Netzwerkmonitor**.
  - **Virtuelle Tastatur** – zeigt die virtuelle Tastatur auf dem Bildschirm an.
- **Sichere Umgebung** – Startet einen sicheren Desktop für die Arbeit mit Programmen, die Ihrer Einschätzung nach gefährlich sein können. Ist der sichere Desktop bereits gestartet, wird zu diesem gewechselt.

  Bei der Arbeit auf dem sicheren Desktop heißt dieser Menüpunkt **Zum normalen Desktop** und dient dazu, zum Standard-Desktop zu wechseln.
- **Kaspersky Internet Security** – Programmhauptfenster öffnen.
- **Schutz anhalten / Schutz fortsetzen** – Echtzeitschutz-Komponenten vorübergehend deaktivieren / wieder aktivieren. Dieser Menüpunkt bezieht sich nicht auf das Programm-Update und die Ausführung von Untersuchungsaufgaben.
- **Kindersicherung aktivieren / Kindersicherung deaktivieren** – aktiviert / deaktiviert die Kindersicherung für das aktuelle Benutzerkonto.
- **Einstellungen** – öffnet das Fenster zur Konfiguration der Einstellungen des Programms.
- **Über das Programm** – Infofenster mit Angaben zum Programm öffnen.
- **Neuigkeiten** – Öffnet das Fenster News Agent (s. Abschnitt "News Agent" auf S. 40). Dieser Menüpunkt wird angezeigt, wenn ungelesene Neuigkeiten vorliegen.

- **Beenden** – Arbeit von Kaspersky Internet Security beenden (bei Auswahl dieses Menüpunkts wird das Programm aus dem Arbeitsspeicher des Computers entladen).

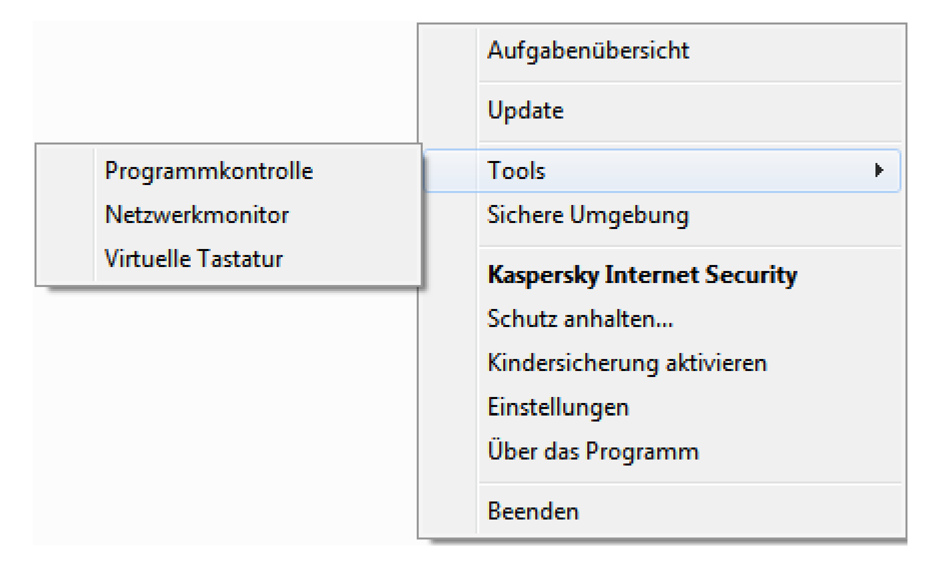


Abbildung 1. Kontextmenü

Wird das Kontextmenü geöffnet, während eine Untersuchungsaufgabe oder Updateaufgabe läuft, so wird ihr Name mit Prozentangabe für das Ausführungsergebnis im Kontextmenü angezeigt. Durch die Auswahl des Menüpunkts mit dem Aufgabennamen gelangen Sie in das Hauptfenster mit einem Bericht über die aktuellen Ausführungsergebnisse.

➧ *Um das Kontextmenü zu öffnen,*

zeigen Sie im Infobereich der Taskleiste mit der Maus auf das Programmsymbol und führen Sie einen Rechtsklick aus.

Unter dem Betriebssystem Microsoft Windows 7 ist das Programmsymbol standardmäßig ausgeblendet. Es lässt sich wieder einblenden, um mit dem Programm zu arbeiten (s. Dokumentation des Betriebssystems).

HAUPTFENSTER VON KASPERSKY INTERNET SECURITY

Die Elemente des Programmhauptfensters bieten Zugriff auf die Hauptfunktionen des Programms.

Das Hauptfenster lässt sich in zwei Bereiche aufteilen:

- Der obere Fensterbereich informiert über den Schutzstatus Ihres Computers.



Der Computer ist sicher

✔ **Bedrohungen:** nicht vorhanden

✔ **Schutzkomponenten:** alle aktiviert

✔ **Datenbanken:** sind veraltet

✔ **Lizenz:** 30 Tage verbleiben

Abbildung 2. Oberer Bereich des Hauptfensters

- Im unteren Fensterbereich können Sie schnell auf die wichtigsten Programmfunktionen zugreifen (z.B. Untersuchungsaufgaben ausführen, Updateaufgabe für Datenbanken und Programm-Module ausführen).

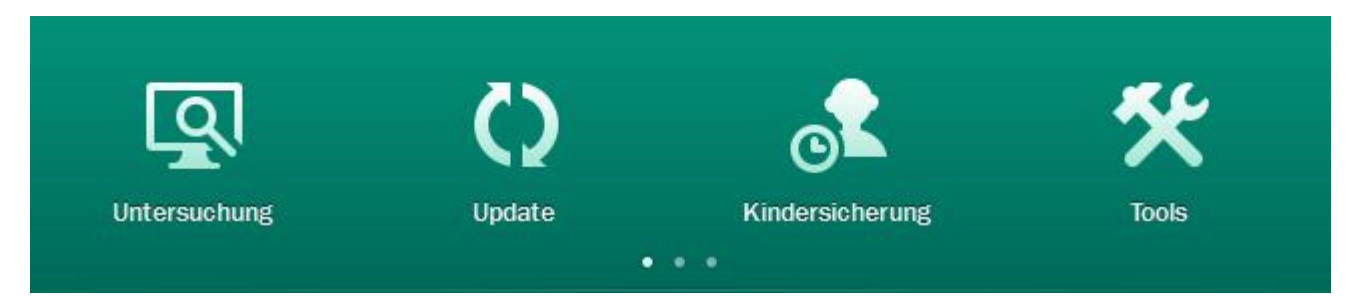


Abbildung 3. Unterer Bereich des Hauptfensters

Wenn im unteren Fensterbereich ein Abschnitt ausgewählt wird, öffnet sich ein Fenster mit der entsprechenden Programmfunktion. Mit der Schaltfläche **Zurück** links oben im Fenster können Sie zur Funktionsauswahl zurückkehren.

Außerdem stehen folgende Schaltflächen und Links zur Verfügung:

- **Cloud-Sicherheit** – Weiter zu Informationen über Kaspersky Security Network (auf S. 184).
- **Einstellungen** – Öffnet das Programmkonfigurationsfenster (s. Abschnitt "Programmkonfigurationsfenster" auf S. 38).
- **Berichte** – Öffnet Berichte über die Programmarbeit.
- **Neuigkeiten** – Öffnet das Fenster von News Agent zum Lesen neuer Nachrichten (s. Abschnitt "News Agent" auf S. 40). Der Link erscheint, nachdem das Programm Neuigkeiten empfangen hat.
- **Hilfe** – zum Hilfesystem für Kaspersky Internet Security wechseln.
- **Mein Kaspersky Account** – Öffnet den persönlichen Bereich des Benutzers auf der Webseite des Technischen Supports.
- **Support** - Das Fenster mit Informationen über das System und mit Links zu Informationsressourcen von Kaspersky Lab (Webseite des Technischen Supports, Forum) öffnen.
- **Lizenzverwaltung** – Geht zur Aktivierung von Kaspersky Internet Security bzw. zur Verlängerung der Lizenz.

➧ *Sie können das Programmhauptfenster auf folgende Weise öffnen:*

- Durch Linksklick auf das Programmsymbol im Infobereich der Taskleiste.

  Unter dem Betriebssystem Microsoft Windows 7 ist das Programmsymbol standardmäßig ausgeblendet. Es lässt sich wieder einblenden, um mit dem Programm zu arbeiten (s. Dokumentation des Betriebssystems).

- Wählen Sie im Kontextmenü den Punkt **Kaspersky Internet Security** (s. Abschnitt "Kontextmenü" auf S. 34).
- Durch Klick auf das Symbol von Kaspersky Internet Security, das sich in der Mitte des Kaspersky Gadgets befindet (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7).

MELDUNGSFENSTER UND POP-UP-MELDUNGEN

Kaspersky Internet Security benachrichtigt Sie mit Hilfe von *Meldungsfenstern* und *Pop-up-Meldungen*, die oberhalb des Programmsymbols im Infobereich der Taskleiste angezeigt werden, über wichtige Ereignisse, die während seiner Ausführung eintreten.

Kaspersky Internet Security zeigt die *Meldungsfenster* immer dann auf dem Bildschirm an, wenn verschiedene Reaktionen auf das Ereignis möglich sind. So können Sie beispielsweise bei Erkennen eines schädlichen Objekts den Zugriff darauf blockieren, dieses löschen oder versuchen, es zu desinfizieren. Das Programm stellt Ihnen die entsprechenden Optionen zu Auswahl. Das Meldungsfenster wird erst dann geschlossen, wenn Sie eine der vorgeschlagenen Optionen auswählen.

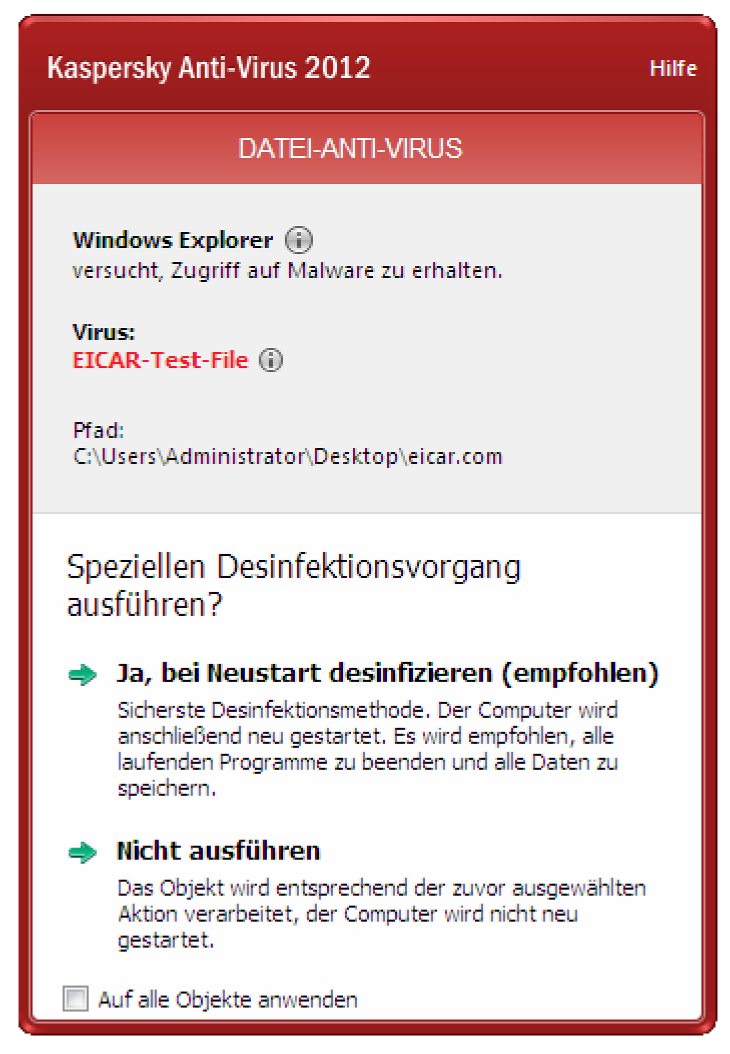


Abbildung 4. Fenster Meldungen

Kaspersky Internet Security zeigt *Pop-up-Fenster* auf dem Bildschirm an, um Sie über Ereignisse zu informieren, die keine Entscheidung Ihrerseits über die weitere Vorgehensweise erfordern. Bestimmte Pop-up-Meldungen enthalten Links, mit denen Sie eine vorgeschlagene Aktion ausführen können (z. B. Update starten oder zur Programmaktivierung wechseln). Pop-up-Meldungen verschwinden nach kurzer Zeit automatisch vom Bildschirm.



Abbildung 5. Pop-up-Meldung

In Abhängigkeit davon, welche Relevanz ein Ereignis für die Computersicherheit besitzt, werden drei Typen von Benachrichtigungen und Pop-up-Meldungen unterschieden:

- Kritische Meldungen informieren über Ereignisse, die vorrangige Priorität für die Computersicherheit besitzen (beispielsweise Fund eines schädlichen Objekts oder einer gefährlichen Aktivität im System). Die Fenster für kritische Meldungen und Pop-up-Fenster sind rot.
- Wichtige Meldungen informieren über Ereignisse, die für die Computersicherheit potenziell wichtig sind (beispielsweise Fund eines möglicherweise infizierten Objekts oder einer verdächtigen Aktivität im System). Die Fenster für wichtige Meldungen und Pop-up-Fenster sind gelb.
- Informative Meldungen informieren über Ereignisse, die keine vorrangige Sicherheitsrelevanz besitzen. Die Fenster für informative Meldungen und Pop-up-Fenster sind grün.

PROGRAMMKONFIGURATIONSFENSTER

Das Konfigurationsfenster von Kaspersky Internet Security dient dazu, die allgemeinen Programmfunktionen, einzelne Schutzkomponenten, Untersuchungs- und Update-Aufgaben anzupassen. Außerdem sind hier erweiterte Einstellungen für andere Aufgaben möglich (s. Abschnitt "Erweiterte Programmeinstellungen" auf S. 66).

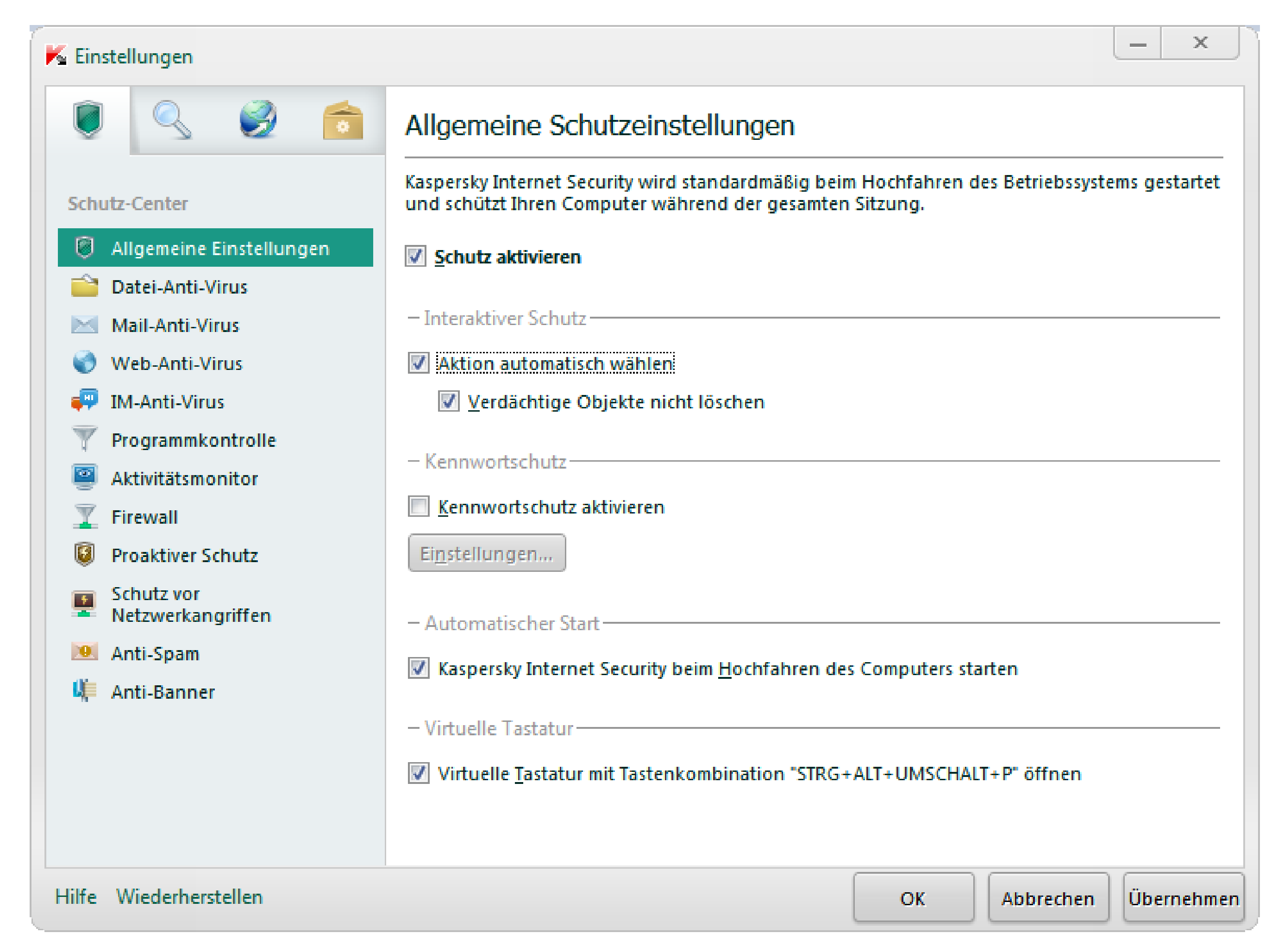


Abbildung 6. Programmkonfigurationsfenster

Das Konfigurationsfenster besteht aus zwei Teilen:

- Im linken Bereich kann eine Programmkomponente, eine Aufgabe oder ein anderes Element gewählt werden, die/das angepasst werden soll.
- Die rechte Fensterseite enthält Steuerelemente, mit denen ein im linken Bereich gewähltes Element angepasst werden kann.

Komponenten, Aufgaben und andere Elemente sind auf der linken Fensterseite in folgende Abschnitte untergliedert:

 – **Schutz-Center**

 – **Untersuchung des Computers**

 – **Update**.

 – **Erweiterte Einstellungen**.

Sie können das Konfigurationsfenster auf folgende Weise öffnen:

- verwenden Sie im oberen Bereich des Programmhauptfensters den Link **Einstellungen** (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 35);
- mit dem Punkt **Einstellungen** im Kontextmenü des Programms (s. Abschnitt "Kontextmenü" auf S. 34);
- durch Klick auf das Symbol **Einstellungen** im Interface des Kaspersky Gadgets (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7). Diese Schaltfläche muss mit der Funktion zum Öffnen des Konfigurationsfensters belegt sein (s. Abschnitt "Kaspersky Gadget verwenden" auf S. 63).

KASPERSKY GADGET

Wenn Kaspersky Internet Security auf einem Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 eingesetzt wird, steht das Kaspersky Gadget zur Verfügung (weiter auch einfach als *Gadget* bezeichnet). Kaspersky Gadget bietet schnellen Zugriff auf die Grundfunktionen des Programms (z.B. Schutzstatus des Computers anzeigen, Objekte auf Viren untersuchen, Programmberichte anzeigen).

Nach der Installation von Kaspersky Internet Security auf einem Computer mit dem Betriebssystem Microsoft Windows 7 erscheint das Gadget automatisch auf dem Desktop. Wenn das Programm auf einem Computer mit dem Betriebssystem Microsoft Windows Vista installiert wird, muss das Gadget manuell zur Sidebar von Microsoft Windows hinzugefügt werden (s. Dokumentation des Betriebssystems).



Abbildung 7. Kaspersky Gadget

NEWS AGENT

Mit Hilfe von *News Agent* werden Sie von Kaspersky Lab über alle wichtigen Ereignisse informiert, die mit Kaspersky Internet Security und generell mit dem Schutz vor Computerbedrohungen zusammenhängen.

Wenn neue Nachrichten eintreffen, werden Sie vom Programm durch das Symbol im Infobereich der Taskleiste (s. unten) und durch eine Pop-up-Meldung benachrichtigt. Außerdem wird die Anzahl der ungelesenen Nachrichten im Programmhauptfenster genannt. Im Gadget für Kaspersky Internet Security erscheint das News-Symbol.

Die Nachrichten können folgendermaßen gelesen werden:

- Durch Klick auf das Symbol im Infobereich der Taskleiste.
- Mit dem Link **Nachrichten lesen** in der News-Pop-up-Meldung.
- Mit dem Link **Nachrichten** im Programmhauptfenster.
- Durch Klick auf das Symbol , das in der Mitte des Gadgets erscheint, wenn neue Nachrichten verfügbar sind (nur für Microsoft Windows Vista und Microsoft Windows 7).

Die aufgezählten Methoden zum Öffnen des Fensters von News Agent sind nur verfügbar, wenn ungelesene Nachrichten vorliegen.

Wenn Sie keine Nachrichten empfangen möchten, können Sie den Empfang von Nachrichten deaktivieren.

PROGRAMM STARTEN UND BEENDEN

Dieser Abschnitt informiert darüber, wie das Programm gestartet und beendet wird.

IN DIESEM ABSCHNITT

AUTOMATISCHEN START AKTIVIEREN UND DEAKTIVIEREN

Unter automatischem Programmstart wird hier der Start von Kaspersky Internet Security verstanden, der ohne Ihr Zutun sofort nach dem Hochfahren des Betriebssystems ausgeführt wird. Diese Startvariante gilt als Standard.

- *Gehen Sie folgendermaßen vor, um den automatischen Start des Programms zu aktivieren oder zu deaktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Allgemeine Einstellungen**.
3. Deaktivieren Sie auf der rechten Fensterseite im Block **Autostart** das Kontrollkästchen **Kaspersky Internet Security beim Hochfahren des Computers starten**, um den automatischen Programmstart auszuschalten. Aktivieren Sie das Kontrollkästchen, um den automatischen Start des Programms einzuschalten:

PROGRAMM MANUELL STARTEN UND BEENDEN

Kaspersky Lab warnt davor, Kaspersky Internet Security zu beenden, da andernfalls der Computer und Ihre persönlichen Daten bedroht sind. Es wird empfohlen, den Computerschutz vorübergehend anzuhalten, ohne das Programm zu beenden.

Kaspersky Internet Security muss manuell gestartet werden, falls Sie den automatischen Programmstart deaktiviert haben (s. Abschnitt "Automatischen Start aktivieren und deaktivieren" auf S. 41).

- *Um das Programm manuell zu starten,*

  wählen Sie im **Startmenü** den Punkt **Programme** → **Kaspersky Internet Security 2012** → **Kaspersky Internet Security 2012**.

- *Um die Arbeit des Programms zu beenden,*

  öffnen Sie durch Rechtsklick das Kontextmenü des Programmsymbols, das sich im Infobereich der Taskleiste befindet, und wählen Sie den Punkt **Beenden**.

  Unter dem Betriebssystem Microsoft Windows 7 ist das Programmsymbol standardmäßig ausgeblendet. Es lässt sich wieder einblenden, um mit dem Programm zu arbeiten (s. Dokumentation des Betriebssystems).

COMPUTERSCHUTZ VERWALTEN

Dieser Abschnitt informiert darüber, wie Bedrohungen für die Computersicherheit erkannt werden und wie die Sicherheitsstufe angepasst wird. Hier finden Sie außerdem Informationen darüber, wie der Schutz während der Arbeit des Programms aktiviert, deaktiviert oder vorübergehend angehalten werden kann.

IN DIESEM ABSCHNITT

PROBLEME IM COMPUTERSCHUTZ DIAGNOSTIZIEREN UND BEHEBEN

Probleme beim Schutz des Computers werden durch den Indikator signalisiert, der sich auf der linken Seite des Programmhauptfensters befindet (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 35). Der Indikator ist ein Monitorabbild, das seine Farbe in Abhängigkeit vom Schutzstatus des Computers ändert: Die Farbe Grün bedeutet, dass der Computer sicher ist. Gelb signalisiert, dass der Schutz Probleme aufweist, und Rot warnt vor einer ernsthaften Bedrohung für die Computersicherheit.



Abbildung 8. Indikator für den Schutzstatus

Probleme und Sicherheitsrisiken sollten umgehend behoben werden.

Durch Klick auf den Indikator im Programmhauptfenster wird das Fenster **Sicherheitsprobleme** geöffnet (s. Abb. unten). Es enthält ausführliche Angaben zum Schutzstatus des Computers und bietet Varianten zum Beheben von Problemen und Bedrohungen.



Abbildung 9. Fenster Sicherheitsprobleme

Die Probleme, die im Schutz vorliegen, sind nach Kategorien angeordnet. Für jedes Problem werden Aktionen genannt, die Sie zur Problemlösung ausführen können.

SCHUTZ AKTIVIEREN UND DEAKTIVIEREN

Kaspersky Internet Security wird in der Grundeinstellung automatisch beim Start des Betriebssystems gestartet und schützt Ihren Computer während der gesamten Sitzung. Alle Schutzkomponenten sind aktiv.

Sie können den Schutz, der von Kaspersky Internet Security gewährleistet wird, vollständig oder teilweise deaktivieren.

Kaspersky Lab warnt davor, den Schutz zu deaktivieren, da dies zur Infektion Ihres Computers und zu Datenverlust führen kann. Es wird empfohlen, den Schutz vorübergehend anzuhalten (s. Abschnitt "Schutz anhalten und fortsetzen" auf S. 44).

Folgende Merkmale informieren darüber, dass der Schutz angehalten oder deaktiviert wurde:

- inaktives (graues) Programmsymbol im Infobereich der Taskleiste (s. Abschnitt "Symbol im Infobereich der Taskleiste" auf S. 33).
- rote Farbe des Sicherheitsindikators im oberen Bereich des Programmhauptfensters.

In diesem Fall wird der Schutz im Kontext der Schutzkomponenten beschrieben. Das Deaktivieren oder Anhalten von Schutzkomponenten übt keinen Einfluss auf die Ausführung von Aufgaben zur Virensuche und zum Update für Kaspersky Internet Security aus.

Der Schutz oder einzelne Programmkomponenten können im Programmkonfigurationsfenster aktiviert oder deaktiviert werden (s. Abschnitt "Programmkonfigurationsfenster" auf S. 38).

Gehen Sie folgendermaßen vor, um den Schutz vollständig zu deaktivieren oder zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Allgemeine Einstellungen**.
3. Deaktivieren Sie das Kontrollkästchen **Schutz aktivieren**, um den Schutz auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um den Schutz einzuschalten.

Gehen Sie folgendermaßen vor, um eine Schutzkomponente zu deaktivieren oder zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente, die aktiviert oder deaktiviert werden soll.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **<Name der Komponente> aktivieren**, um die Komponente auszuschalten. Aktivieren Sie dieses Kontrollkästchen, um die Komponente einzuschalten.

SCHUTZ ANHALTEN UND FORTSETZEN

Das Anhalten des Schutzes bedeutet, dass alle Komponenten für einen bestimmten Zeitraum ausgeschaltet werden.

Folgende Merkmale informieren darüber, dass der Schutz angehalten oder deaktiviert wurde:

- inaktives (graues) Programmsymbol im Infobereich der Taskleiste (s. Abschnitt "Symbol im Infobereich der Taskleiste" auf S. 33).
- rote Farbe des Sicherheitsindikators im oberen Bereich des Programmhauptfensters.

In diesem Fall wird der Schutz im Kontext der Schutzkomponenten beschrieben. Das Deaktivieren oder Anhalten von Schutzkomponenten übt keinen Einfluss auf die Ausführung von Aufgaben zur Virensuche und zum Update für Kaspersky Internet Security aus.

Wenn im Augenblick, als der Schutz beendet wurde, auf dem Computer Netzwerkverbindungen vorhanden waren, erscheint auf dem Bildschirm eine Meldung darüber, dass diese Verbindungen getrennt werden.

Auf einem Computer mit Microsoft Windows Vista oder Microsoft Windows 7 kann der Schutz mit Hilfe des Kaspersky Gadgets angehalten werden. Dazu muss eine der Gadget-Schaltflächen mit der Funktion zum Anhalten des Schutzes belegt sein (s. Abschnitt "Kaspersky Gadget verwenden" auf S. 63).

Gehen Sie folgendermaßen vor, um den Computerschutz anzuhalten:

1. Öffnen Sie das Fenster **Schutz anhalten**. Dafür gibt es unterschiedliche Möglichkeiten:

- Wählen Sie im Kontextmenü des Programmsymbols den Punkt **Schutz anhalten** (s. Abschnitt "Kontextmenü" auf S. 34).
- Klicken Sie im Interface des Kaspersky Gadgets auf die Schaltfläche mit dem Symbol **Schutz anhalten** (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7).

2. Wählen Sie im Fenster **Schutz anhalten** den Zeitraum, nach dem der Schutz wieder aktiviert werden soll:
   - **Anhalten für...** – Der Schutz wird nach Ablauf des Zeitraums wieder aktiviert, der in der Dropdown-Liste festgelegt wird.
   - **Anhalten bis zum Neustart** – Der Schutz wird nach dem Neustart des Programms oder des Systems aktiviert (unter der Bedingung, dass der automatische Programmstart aktiviert ist (s. Abschnitt "Automatischen Start aktivieren und deaktivieren"auf S. 41)).
   - **Anhalten** – Der Schutz wird wieder aktiviert, wenn Sie ihn fortsetzen (s. unten).

➧ *Um den Computerschutz fortzusetzen,*

wählen Sie im Kontextmenü des Programmsymbols den Punkt **Schutz fortsetzen** (s. Abschnitt "Kontextmenü" auf S. 34).

Der Computerschutz kann auf diese Weise fortgesetzt werden, wenn die Variante **Anhalten**, **Anhalten für...** oder **Anhalten bis zum Neustart** gewählt wurde.

LÖSUNGEN FÜR TYPISCHE AUFGABEN

Dieser Abschnitt informiert darüber, wie mit diesem Programm grundlegende Aufgaben für den Computerschutz gelöst werden.

IN DIESEM ABSCHNITT

WIE DAS PROGRAMM AKTIVIERT WIRD

Durch die *Aktivierung* erlangt die Lizenz für die Nutzung der Vollversion des Programms ihre Gültigkeit für den entsprechenden Zeitraum.

Wenn Sie das Programm nicht bei der Installation aktiviert haben, können Sie dies später nachholen. Falls eine Programmaktivierung notwendig ist, werden Sie von Kaspersky Internet Security durch entsprechende Meldungen im Infobereich der Taskleiste daran erinnert.

Gehen Sie folgendermaßen vor, um den Aktivierungsassistenten für Kaspersky Internet Security zu starten:

- Klicken Sie im Meldungsfenster von Kaspersky Internet Security, das im Infobereich der Taskleiste erscheint, auf den Link **Bitte aktivieren Sie das Programm**.
- Verwenden Sie im unteren Bereich des Programmhauptfensters den Link **Aktivierungscode eingeben**. Klicken Sie im folgenden Fenster **Lizenzverwaltung** auf **Programm aktivieren**.

Im Aktivierungsassistenten für das Programm sind eine Reihe von Einstellungen erforderlich.

Schritt 1. Aktivierungscode eingeben

Tragen Sie im entsprechenden Feld den Aktivierungscode ein und klicken Sie auf **Weiter**.

Schritt 2. Aktivierungsanfrage

Nach einer erfolgreichen Aktivierungsabfrage geht der Assistent automatisch zum nächsten Schritt.

Schritt 3. Anmeldedaten eingeben

Eine Anmeldung ist erforderlich, damit sich der Benutzer künftig an den Technischen Support wenden kann. Nicht registrierte Benutzer werden hier kurz aufgehalten.

Geben Sie Ihre Anmeldedaten an und klicken Sie dann auf **Weiter**.

Schritt 4. Aktivierung

Wenn die Programmaktivierung erfolgreich verlaufen ist, geht der Assistent automatisch zum nächsten Fenster.

Schritt 5. Assistent abschließen

Dieses Fenster des Assistenten informiert über die Aktivierungsergebnisse: Typ und Gültigkeitsdauer der verwendeten Lizenz.

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

LIZENZERWERB ODER -VERLÄNGERUNG

Wenn Sie Kaspersky Internet Security installiert haben und keine Lizenz besitzen, können Sie nach der Programminstallation eine Lizenz erwerben. Beim Kauf einer Lizenz erhalten Sie einen Aktivierungscode, mit dem das Programm aktiviert werden muss (s. Abschnitt "Wie das Programm aktiviert wird" auf S. 46).

Wenn die Gültigkeit einer Lizenz bald abläuft, können Sie diese verlängern. Sie können eine neue Lizenz erwerben und müssen nicht bis zum Ablauf des momentan verwendeten Aktivierungscodes warten. Dazu muss ein Reserve-Aktivierungscode hinzugefügt werden. Wenn die verwendete Lizenz abläuft, wird Kaspersky Internet Security automatisch mit dem Reserve-Aktivierungscode aktiviert.

Gehen Sie folgendermaßen vor, um eine Lizenz zu erwerben:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf den Link **Lizenzverwaltung**, der sich im unteren Bereich des Programmhauptfensters befindet, um das Fenster **Lizenzverwaltung** zu öffnen.
3. Klicken Sie im folgenden Fenster auf **Aktivierungscode kaufen**.

   Die Webseite des Online-Shops wird geöffnet. Dort können Sie eine Lizenz erwerben.

Gehen Sie folgendermaßen vor, um einen Aktivierungscode hinzuzufügen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie auf den Link **Lizenzverwaltung**, der sich im unteren Bereich des Programmhauptfensters befindet, um das Fenster **Lizenzverwaltung** zu öffnen.

   Das Fenster **Lizenzverwaltung** wird geöffnet.
3. Klicken Sie im folgenden Fenster unter **Reserve-Aktivierungscode** auf **Aktivierungscode eingeben**.

   Der Assistent zur Programmaktivierung wird geöffnet.
4. Tragen Sie in die entsprechenden Felder den Aktivierungscode ein und klicken Sie auf **Weiter**.

   Kaspersky Internet Security schickt die Daten zur Überprüfung an den Aktivierungsserver. Wenn die Überprüfung erfolgreich verläuft, geht der Assistent automatisch weiter zum nächsten Fenster.
5. Wählen Sie die Variante **Als Reservecode verwenden** und klicken Sie auf **Weiter**.
6. Klicken bei Abschluss des Assistenten auf **Beenden**.

AUF MELDUNGEN DES PROGRAMMS REAGIEREN

Meldungen, die das Programm im Infobereich der Taskleiste anzeigt, informieren über Ereignisse bei der Arbeit des Programms und erfordern Ihre Aufmerksamkeit. In Abhängigkeit von der Priorität eines Ereignisses sind folgende Arten von Meldungen möglich:

- Kritische Meldungen informieren über Ereignisse, die vorrangige Priorität für die Computersicherheit besitzen (beispielsweise Fund eines schädlichen Objekts oder einer gefährlichen Aktivität im System). Die Fenster für kritische Meldungen und Pop-up-Fenster sind rot.
- Wichtige Meldungen informieren über Ereignisse, die für die Computersicherheit potenziell wichtig sind (beispielsweise Fund eines möglicherweise infizierten Objekts oder einer verdächtigen Aktivität im System). Die Fenster für wichtige Meldungen und Pop-up-Fenster sind gelb.
- Informative Meldungen informieren über Ereignisse, die keine vorrangige Sicherheitsrelevanz besitzen. Die Fenster für informative Meldungen und Pop-up-Fenster sind grün.

Wenn eine Benachrichtigung auf dem Bildschirm erscheint, muss eine der vorgegebenen Varianten ausgewählt werden. Als optimal gilt die von Kaspersky Lab empfohlene Variante.

AKTUALISIERUNG VON PROGRAMMDATENBANKEN UND -MODULEN

Kaspersky Internet Security überprüft in der Grundeinstellung automatisch, ob auf den Kaspersky-Lab-Updateservern neue Updates vorhanden sind. Wenn auf dem Server neue Updates vorhanden sind, lädt Kaspersky Internet Security die Updates im Hintergrundmodus herunter und installiert sie. Sie können das Update von Kaspersky Internet Security jederzeit manuell starten.

Um Updates von den Kaspersky-Lab-Servern herunterzuladen, ist eine Internetverbindung erforderlich.

Um das Update aus dem Kontextmenü zu starten,

wählen Sie im Kontextmenü des Programmsymbols den Punkt **Update**.

Gehen Sie folgendermaßen vor, um das Update aus dem Hauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie im unteren Fensterbereich den Abschnitt **Update**.
2. Klicken Sie im folgenden Fenster **Update** auf **Aktualisieren**.

WIE WICHTIGE COMPUTERBEREICHE AUF VIREN UNTERSUCHT WERDEN.

Die Untersuchung wichtiger Bereiche umfasst folgende Objekte:

- Objekte, die beim Hochfahren des Betriebssystems geladen werden.
- Systemspeicher
- Laufwerksbootsektoren
- Objekte, die vom Benutzer hinzugefügt wurden (s. Abschnitt "Liste der Untersuchungsobjekte erstellen" auf S. 72).

Sie können die Untersuchung der wichtigen Bereiche auf folgende Weise starten:

- mit einer zuvor hergestellten Verknüpfung (s. S. 76).
- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 35)

Gehen Sie folgendermaßen vor, um die Untersuchung mit Hilfe einer Verknüpfung zu starten:

1. Öffnen Sie das Explrer-Fenster von Windows Explorer und gehen Sie in den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie die Untersuchung durch Doppelklick auf die Verknüpfung.

Gehen Sie folgendermaßen vor, um die Untersuchung aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie im unteren Fensterbereich den Abschnitt **Untersuchung**.
2. Klicken Sie im folgenden Fenster **Untersuchung** im Block **Untersuchung wichtiger Bereiche** auf die Schaltfläche .

UNTERSUCHUNG VON DATEIEN, ORDNERN, LAUFWERKEN UND ANDEREN OBJEKTEN AUF VIREN

Ein bestimmtes Objekt kann folgendermaßen auf Viren untersucht werden:

- mit Hilfe des Kontextmenüs für ein Objekt
- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 35)
- mit Hilfe des Gadgets von Kaspersky Internet Security (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7).

➡ *Gehen Sie folgendermaßen vor, um eine Untersuchungsaufgabe aus dem Kontextmenü eines Objekts zu starten:*

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und gehen Sie in den Ordner mit dem Untersuchungsobjekt.

2. Öffnen Sie durch Rechtsklick das Kontextmenü für das Objekt (s. Abb. unten) und wählen Sie den Punkt **Auf Viren untersuchen**.

   Der Fortschritt und das Ergebnis der Aufgabenausführung werden im Fenster **Aufgabenübersicht** angezeigt.

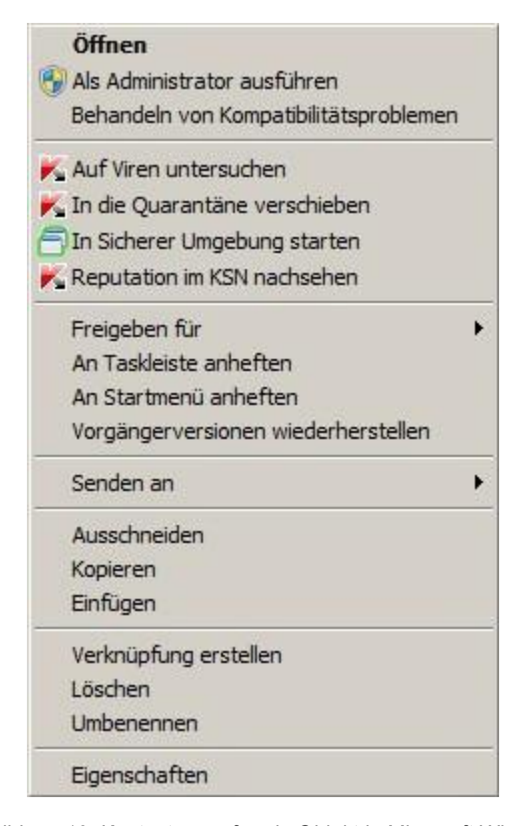


Abbildung 10. Kontextmenü für ein Objekt in Microsoft Windows

➡ *Gehen Sie folgendermaßen vor, um die Untersuchung eines Objekts aus dem Programmhauptfenster zu starten:*

1. Öffnen Sie das Programmhauptfenster und wählen Sie im unteren Fensterbereich den Abschnitt **Untersuchung**.

2. Verwenden Sie eine der folgenden Methoden, um ein Untersuchungsobjekt anzugeben:

   - Öffnen Sie mit dem Link **auswählen**, der sich im rechten Fensterbereich befindet, das Fenster **Benutzerdefinierte Untersuchung** und aktivieren Sie die Kontrollkästchen für die Ordner und Laufwerke, die untersucht werden sollen.

     Gehen Sie folgendermaßen vor, wenn ein Objekt, das untersucht werden soll, nicht in diesem Fenster vorhanden ist:

     a. Klicken Sie auf **Hinzufügen**.

     b. Wählen Sie im folgenden Fenster **Untersuchungsobjekt wählen** ein Untersuchungsobjekt.

   - Ziehen Sie ein Untersuchungsobjekt mit der Maus in den dafür vorgesehenen Bereich des Hauptfensters (s. Abb. unten).

Der Fortschritt der Aufgabenausführung wird im folgenden Fenster **Aufgabenübersicht** dargestellt.



Abbildung 11. Bereich im Fenster Untersuchung, in den ein Untersuchungsobjekt gezogen werden muss

➡ *Um ein Objekt mit Hilfe des Gadgets auf Viren zu untersuchen,*

ziehen Sie das Untersuchungsobjekt auf das Gadget.

➡ *Der Fortschritt der Aufgabenausführung wird im Fenster **Aufgabenübersicht** dargestellt..*

WIE EINE VOLLSTÄNDIGE VIRENUNTERSUCHUNG DES COMPUTERS AUSGEFÜHRT WIRD.

Eine vollständige Virenuntersuchung kann folgendermaßen gestartet werden:

- mit einer zuvor hergestellten Verknüpfung (s. S. 76).
- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 35)

➡ *Gehen Sie folgendermaßen vor, um die vollständige Untersuchung mit Hilfe einer Verknüpfung zu starten:*

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie die Untersuchung durch Doppelklick auf die Verknüpfung.

➡ *Gehen Sie folgendermaßen vor, um die vollständige Untersuchung aus dem Programmhauptfenster zu starten:*

1. Öffnen Sie das Programmhauptfenster und wählen Sie unten im Fenster den Abschnitt **Untersuchung**.
2. Klicken Sie im folgenden Fenster **Untersuchung** im Block **Vollständige Untersuchung** auf die Schaltfläche ▶.

WIE DER COMPUTER AUF SCHWACHSTELLEN UNTERSUCHT WIRD.

Schwachstellen sind Teile eines Programmcodes, den Angreifer für ihre Ziele nutzen können, um beispielsweise Daten zu kopieren, die von Programmen mit ungeschütztem Code verwendet werden. Die Untersuchung Ihres Computers auf potenzielle Schwachstellen erlaubt es, solche "Schwachpunkte" im Schutz des Rechners zu finden. Erkannte Schwachstellen sollten beseitigt werden.

Sie können die Schwachstellensuche auf folgende Weise starten:

- aus dem Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 35)
- mit einer zuvor hergestellten Verknüpfung (s. S. 76)

Gehen Sie folgendermaßen vor, um die Aufgabe mit Hilfe einer Verknüpfung zu starten:

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und öffnen Sie den Ordner, in dem Sie die Verknüpfung erstellt haben.
2. Starten Sie die Aufgabe zur Schwachstellensuche durch Doppelklick auf die Verknüpfung.

Gehen Sie folgendermaßen vor, um die Aufgabe aus dem Programmhauptfenster zu starten:

1. Öffnen Sie das Programmhauptfenster und wählen Sie im unteren Fensterbereich den Abschnitt **Untersuchung**.
2. Klicken Sie im folgenden Fenster **Untersuchung** im Block **Schwachstellensuche** auf die Schaltfläche .

WIE IHRE PERSÖNLICHEN DATEN VOR DIEBSTAHL GESCHÜTZT WERDEN.

Mit Kaspersky Internet Security können Sie Ihre persönlichen Daten vor einem Diebstahl durch Angreifer schützen. Zu diesen Daten zählen beispielsweise:

- Kennwörter, Benutzernamen und andere Anmeldedaten
- Konto- und Kreditkartennummern

Kaspersky Internet Security bietet folgende Komponenten und Tools, die dem Schutz Ihrer persönlichen Daten dienen:

- Anti-Phishing. Schützt vor Datendiebstahl durch Phishing.
- Virtuelle Tastatur. Verhindert das Abfangen von über die Tastatur eingegebenen Daten.
- Kindersicherung (s. S. 152). Beschränkt das Senden von persönlichen Daten über das Internet.

IN DIESEM ABSCHNITT

SCHUTZ VOR PHISHING

Für den Schutz vor Phishing ist Anti-Phishing verantwortlich, das zu den Komponenten Web-Anti-Virus, Anti-Spam und IM-Anti-Virus gehört. Kaspersky Lab empfiehlt, die Phishing-Prüfung für alle Komponenten zu aktivieren.

Gehen Sie folgendermaßen vor, um den Phishing-Schutz für Web-Anti-Virus zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Das Fenster **Web-Anti-Virus** wird geöffnet.
5. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Links untersuchen** das Kontrollkästchen **Webseiten auf Phishing prüfen**.

Gehen Sie folgendermaßen vor, um den Phishing-Schutz für IM-Anti-Virus zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich
3. im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.
4. Aktivieren Sie auf der rechten Fensterseite im Block **Untersuchungsmethoden** das Kontrollkästchen **Links mit Datenbank für Phishing-Webadressen untersuchen**.

Gehen Sie folgendermaßen vor, um den Phishing-Schutz für Anti-Spam zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie im linken Fensterbereich im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Mit Phishing-Elementen**.

SCHUTZ VOR DEM ABFANGEN VON TASTATUREINGABEN

Bei der Arbeit im Internet ist es häufig erforderlich, persönliche Daten, Benutzername und Kennwort einzugeben. Beispiele sind die Anmeldung auf Webseiten, der Besuch von Online-Shops und die Verwendung von Online-Banking.

In solchen Situationen besteht die Gefahr, dass persönliche Informationen mit Hilfe von Hardware-Hooks oder mit Keyloggern (Programme, die Tasteneingaben registrieren) abgefangen werden.

Die Virtuelle Tastatur ermöglicht es, das Abfangen von über die Tastatur eingegebenen Daten zu verhindern.

Die Virtuelle Tastatur kann Ihre persönlichen Daten nicht schützen, wenn eine Webseite gehackt wurde und die Eingabe solcher Daten fordert, da die Informationen in diesem Fall dem Angreifer direkt in die Hände fallen.

Viele Spyware-Programme besitzen Funktionen zum Anlegen von Screenshots, die an Angreifer für Analyse und Sammeln von persönlichen Benutzerdaten automatisch übergeben werden. Die Virtuelle Tastatur schützt davor, dass persönliche Daten durch das Anlegen von Bildschirmkopien (Screenshots) abgefangen werden.

Die Virtuelle Tastatur schützt persönliche Daten nur dann vor Diebstahlversuchen, wenn Sie den Internetbrowser Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome verwenden.

Die Virtuelle Tastatur besitzt folgende Besonderheiten:

- Die Betätigung der Tasten der virtuellen Tastatur erfolgt durch Mausklick.
- Im Gegensatz zu einer echten Tastatur ist es auf der Virtuellen Tastatur nicht möglich, mehrere Tasten gleichzeitig zu drücken. Um Tastenkombinationen zu verwenden (z.B. **ALT+F4**), ist es deshalb notwendig,

zuerst die erste Taste (z.B. **ALT**), dann die zweite Taste (z.B. **F4**) und anschließend erneut die erste Taste zu drücken. Das wiederholte Drücken ersetzt das Loslassen einer Taste auf der echten Tastatur.

- Auf der Virtuellen Tastatur wird die Eingabesprache mit dem Tastenkürzel **STRG+UMSCHALT** geändert (wobei mit der rechten Maustaste auf die Taste **Umschalt** gedrückt wird) oder mit **STRG+NACH LINKS ALT** (wobei mit der rechten Maustaste auf **NACH LINKS ALT** gedrückt wird). Die Kombination ist von den festgelegten Einstellungen abhängig.

Die Virtuelle Tastatur kann auf folgende Weise geöffnet werden:

- aus dem Kontextmenü des Programms
- aus dem
- aus dem Fenster des Browsers Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome
- mit Hilfe einer Tastenkombination.

➡ *Um die Virtuelle Tastatur vom Kontextmenü aus zu öffnen,*

wählen Sie im Kontextmenü des Programmsymbols den Punkt **Tools** →**Virtuelle Tastatur**.

➡ *Um die virtuelle Tastatur aus dem Hauptfenster des Programms zu öffnen,*

wählen Sie unten im Hauptfenster den Abschnitt **Virtuelle Tastatur**.

➡ *Um die virtuelle Tastatur von einem Browserfenster aus zu öffnen,*

klicken Sie in der Symbolleiste von Microsoft Internet Explorer, Mozilla Firefox oder Google Chrome auf die Schaltfläche **Virtuelle Tastatur**.

➡ *Um die virtuelle Tastatur mit Hilfe der Computertastatur zu öffnen,*

betätigen Sie die Tastenkombination **STRG+ALT+UMSCHALT+P**.

VERTRAULICHE DATEN SCHÜTZEN, DIE AUF WEBSEITEN EINGEGEBEN WERDEN

Zum Schutz vertraulicher Daten, die Sie auf Webseiten eingeben (beispielsweise Kreditkartennummern, Kennwörter für Online-Banking), schlägt Kaspersky Internet Security vor, solche Seiten im Sicheren Browser zu öffnen.

Sie können die Zugriffskontrolle für Online-Banking-Dienste aktivieren (s. Abschnitt "Zugriff auf Online-Banking-Dienste kontrollieren" auf S. 100), damit Banking-Webseiten automatisch erkannt werden. Außerdem können Sie den Sicheren Browser manuell starten.

Der Sichere Browser kann auf folgende Weise gestartet werden:

- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 35).
- mit Hilfe einer Verknüpfung auf dem Desktop (s. Abschnitt "Verknüpfung auf dem Desktop erstellen" auf S. 149).

➡ *Gehen Sie folgendermaßen vor, um den Sicheren Browser aus dem Hauptfenster von Kaspersky Internet Security zu starten:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Sichere Umgebung** aus.

3. Klicken Sie im folgenden Fenster auf **Sicheren Browser starten**.

WAS TUN, WENN SIE VERMUTEN, DASS EIN OBJEKT VON EINEM VIRUS INFIZIERT IST?

Wenn Sie den Verdacht haben, dass ein Objekt infiziert ist, sollten Sie es mit Hilfe von Kaspersky Internet Security untersuchen (s. Abschnitt "Untersuchung von Dateien, Ordnern, Laufwerken und anderen Objekten auf Viren" auf S. 49).

Wenn ein Objekt bei der Untersuchung vom Programm als virenfrei eingestuft wird, Sie aber vermuten, dass es infiziert ist, stehen folgende Aktionen zur Auswahl:

- Objekt in die *Quarantäne* verschieben. Objekte, die in die Quarantäne verschoben wurden, stellen keine Gefahr für Ihren Computer dar. Möglicherweise kann die Bedrohung eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken von Kaspersky Internet Security aktualisiert wurden.
- Objekt an das *Virenlabor* schicken. Die Experten des Virenlabors untersuchen das Objekt. Falls es tatsächlich infiziert ist, wird den Datenbanken eine Beschreibung des neuen Virus hinzugefügt. Die Datenbanken werden beim Update vom Programm aktualisiert (s. Abschnitt "Datenbanken und Programm-Module aktualisieren" auf S. 48).

Eine Datei kann auf zwei Arten in die Quarantäne verschoben werden:

- mit der Schaltfläche **In die Quarantäne verschieben** im Fenster **Quarantäne**
- mit Hilfe des Kontextmenüs für die Datei.

➨ *Um eine Datei aus dem Fenster Quarantäne in die Quarantäne zu verschieben, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Quarantäne**.
3. Klicken Sie auf der Registerkarte **Quarantäne** auf die Schaltfläche **In die Quarantäne verschieben**.
4. Wählen Sie im folgenden Fenster die Datei, die in die Quarantäne verschoben werden soll.

➨ *Gehen Sie folgendermaßen vor, um eine Datei mit Hilfe des Kontextmenüs in die Quarantäne zu verschieben:*

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und gehen Sie in den Ordner mit der Datei, die in die Quarantäne verschoben werden soll.

Öffnen Sie durch Rechtsklick das Kontextmenü für die Datei und wählen Sie den Punkt **In die Quarantäne verschieben**.

➨ *Gehen Sie folgendermaßen vor, um eine Datei an das Virenlabor zu schicken:*

1. Gehen Sie auf die Seite, die zum Senden einer Anfrage an das Virenlabor dient (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de).
2. Folgen Sie den Anweisungen, die auf dieser Seite gegeben werden, um eine Anfrage zu schicken.

UNBEKANNTES PROGRAMM STARTEN, OHNE DASS DAS SYSTEM GEFÄHRDET WIRD

Es wird empfohlen, Programme, an deren Sicherheit Sie zweifeln, in der Sicheren Umgebung zu starten.

Die Sichere Umgebung ist vom Betriebssystem des Computers isoliert. Bei der Arbeit in der Sicheren Umgebung werden Objekte, die tatsächlich zum Betriebssystem gehören, nicht verändert. Deshalb haben die Aktionen eines infizierten Programms keinen Einfluss auf das Betriebssystem, wenn Sie es in der Sicheren Umgebung starten.

Sie können die Sichere Umgebung als separaten Desktop starten (s. S. 146) oder ein bestimmtes Programm im sicheren Modus auf dem normalen Desktop starten.

Für Programme, die im sicheren Modus auf dem normalen Desktop gestartet wurden, besitzt das Programmfenster einen grünen Rahmen. Außerdem besitzen die Programme in der Liste der Programme, die von Programmkontrolle kontrolliert werden (s. Abschnitt "Programmkontrolle107" auf S.), ein Merkmal für den sicheren Start.

Nachdem ein Programm abgeschlossen wurde, werden automatisch alle Veränderungen rückgängig gemacht, die im Laufe des Programms vorgenommen wurden.

➡ *Um ein Programm vom Kontextmenü für Microsoft Windows im sicheren Modus zu starten,*

öffnen Sie durch Rechtsklick das Kontextmenü für das ausgewählte Objekt (Verknüpfung oder ausführbare Programmdatei) und wählen Sie den Punkt **In Sicherer Umgebung starten**.

WIE MIT EINER GROßEN ANZAHL VON SPAM-MAILS VERFAHREN WIRD?

Falls Sie viel Spam erhalten, aktivieren Sie die Komponente Anti-Spam und wählen Sie die empfohlene Sicherheitsstufe.

➡ *Gehen Sie folgendermaßen vor, um Anti-Spam zu aktivieren und die empfohlene Sicherheitsstufe zu wählen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Anti-Spam aktivieren**.
4. Vergewissern Sie sich, dass im Block **Sicherheitsstufe** die Sicherheitsstufe **Empfohlen** ausgewählt ist.

   Sollte die Sicherheitsstufe **Niedrig** oder **Benutzerdefiniert** gewählt sein, so klicken Sie auf **Standard**. Die Sicherheitsstufe erhält automatisch den Wert **Empfohlen**.

WAS TUN, WENN SIE VERMUTEN, DASS IHR COMPUTER INFIZIERT IST?

Wenn Sie vermuten, dass das Betriebssystem Ihres Computers durch Malware-Aktivitäten oder Systemfehler beschädigt worden ist, verwenden Sie den *Systemwiederherstellungs-Assistenten*, der die Spuren von schädlichen Objekten im System beseitigt. Die Kaspersky-Lab-Experten empfehlen außerdem, den Assistenten nach einer Desinfektion des Computers auszuführen, um sicherzustellen, dass alle aufgetretenen Bedrohungen und Beschädigungen beseitigt wurden.

Der Wiederherstellungs-Assistent prüft das System auf Veränderungen und Beschädigungen (z.B. veränderte Dateierweiterungen, Blockierung der Netzwerkumgebung und der Systemsteuerung). Veränderungen und Beschädigungen können folgende Gründe haben: Aktivität schädlicher Programme, fehlerhafte Systemeinstellungen, Systemfehler oder Verwendung von fehlerhaft funktionierenden Systemoptimierungsprogrammen.

Nach der Untersuchung analysiert der Assistent die gesammelten Informationen, um festzustellen, ob im System Beschädigungen vorliegen, die sofort behoben werden müssen. Aufgrund der Untersuchungsergebnisse wird eine Liste von Aktionen erstellt, die ausgeführt werden müssen, um die Beschädigungen zu beheben. Der Assistent ordnet die Aktionen nach der Priorität der gefundenen Probleme in Kategorien an.

Gehen Sie folgendermaßen vor, den Systemwiederherstellungs-Assistenten zu starten:

1. Öffnen Sie das Programmhauptfenster (s. S. 35).
2. Wählen Sie im unteren Bereich des Fensters den Abschnitt **Tools**.
3. Klicken Sie im folgenden Fenster im Block **Wiederherstellung nach Infektion** auf **Ausführen**.

   Das Fenster des Systemwiederherstellungs-Assistenten wird geöffnet.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Schritt 1. Systemwiederherstellung starten

Vergewissern Sie sich, dass im Assistentenfenster die Variante **Suche nach Problemen, die mit Malware-Aktivität zusammenhängen, durchführen** gewählt wurde, und klicken Sie auf **Weiter**.

Schritt 2. Nach Problemen suchen

Der Assistent sucht nach Problemen und möglichen Beschädigungen, die behoben werden müssen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für die Problembehebung wählen

Alle Beschädigungen, die beim vorherigen Schritt gefunden wurden, werden ihrer Gefährlichkeit nach angeordnet. Für jede Gruppe von Beschädigungen schlagen die Kaspersky-Lab-Spezialisten eine Auswahl von Aktionen vor, deren Ausführung die Beschädigungen beheben kann. Die Aktionen sind in drei Gruppen unterteilt:

- *Ausdrücklich empfohlene Aktionen* können Beschädigungen beheben, die ein ernsthaftes Problem darstellen. Es wird empfohlen, alle Aktionen dieser Gruppe auszuführen.
- *Empfohlene Aktionen* dienen zum Beheben von Beschädigungen, die ein potenzielles Risiko darstellen können. Es wird empfohlen, auch alle Aktionen dieser Gruppe auszuführen.
- *Zusätzliche Aktionen* dienen dazu, momentan ungefährliche Beschädigungen des Systems zu beheben, die die Computersicherheit in Zukunft bedrohen können.

Klicken Sie links vom Namen einer Gruppe auf das Zeichen **+**, um die Aktionen der Gruppe anzuzeigen.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen.

Die standardmäßig aktivierten Kontrollkästchen sollten auf keinen Fall entfernt werden, da hierdurch die Sicherheit Ihres Computers bedroht wird.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Probleme beheben

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Die Problembehebung kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Problembehebung automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

WIE EINE DATEI WIEDERHERGESTELLT WIRD, DAS VOM PROGRAMM GELÖSCHT ODER DESINFIZIERT WURDE.

Kaspersky Lab warnt davor, gelöschte und desinfizierte Dateien wiederherzustellen, da diese eine Gefahr für Ihren Computer darstellen können.

Wenn die Wiederherstellung einer gelöschten oder desinfizierten Datei erforderlich ist, verwenden Sie dazu die Sicherungskopie, die vom Programm bei der Untersuchung angelegt wurde.

Gehen Sie folgendermaßen vor, um eine Datei wiederherzustellen, die vom Programm gelöscht oder desinfiziert wurde:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Quarantäne**.
3. Wählen Sie auf der Registerkarte **Backup** in der Liste die entsprechende Datei aus und klicken Sie auf **Wiederherstellen**.

WIE EINE NOTFALL-CD ERSTELLT UND VERWENDET WIRD.

Es wird empfohlen, eine Notfall-CD zu erstellen, nachdem Kaspersky Internet Security installiert und der Computer untersucht wurde.

Eine Notfall-CD besteht aus dem Programm Notfall-CD, das auf einem Wechseldatenträger gespeichert ist (CD oder USB-Gerät).

Die Notfall-CD kann später verwendet werden, um den infizierten Computer zu untersuchen und zu desinfizieren, wenn eine Desinfektion mit anderen Mitteln (z.B. Antiviren-Programmen) fehlschlägt.

IN DIESEM ABSCHNITT

NOTFALL-CD ERSTELLEN

Beim Anlegen einer Notfall-CD wird ein Disk-Abbild (Datei im ISO-Format) mit einer aktuellen Version des Programms Notfall-CD erstellt und auf einen Wechseldatenträger gespeichert.

Ein Original des Disk-Abbilds kann vom Kaspersky-Lab-Server heruntergeladen oder aus einer lokalen Quelle kopiert werden.

Eine Notfall-CD wird mit dem *Notfall-CD-Assistenten* erstellt. Die vom Assistenten angelegte Abbild-Datei rescuecd.iso wird auf der Festplatte Ihres Computers gespeichert:

- im Betriebssystem Microsoft Windows XP – im Ordner Dokumente und Einstellungen\All Users\Anwendungsdaten\Kaspersky Lab\AVP12\Data\Rdisk\.
- in Betriebssystemen Microsoft Windows Vista und Microsoft Windows 7 – im Ordner Benutzer\Kaspersky Lab\AVP12\Data\Rdisk\.

Gehen Sie folgendermaßen vor, um eine Notfall-CD zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Bereich des Fensters den Abschnitt **Tools**.
3. Klicken Sie im folgenden Fenster im Block **Notfall-CD** auf **Erstellen**.
4. Das Fenster **Notfall-CD-Assistent** wird geöffnet.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Details zu den einzelnen Schritten des Assistenten

Schritt 1. Assistent starten. Suche nach einem existierenden Festplattenabbild

Das erste Fenster des Assistenten informiert über das Programm Notfall-CD.

Wenn der Assistent in dem dafür vorgesehenen Ordner (s. oben) ein früher erstelltes Notfall-CD-Abbild findet, wird im ersten Fenster des Assistenten das Kontrollkästchen **Vorhandenes Abbild verwenden** angezeigt. Aktivieren Sie dieses Kontrollkästchen, um die gefundene Datei als Grundlage für das Disk-Abbild zu verwenden und direkt zum Schritt **Abbild-Datei aktualisieren** weiterzugehen (s. unten). Deaktivieren Sie dieses Kontrollkästchen, wenn Sie das gefundene Disk-Abbild nicht verwenden möchten. Der Assistent geht weiter zum Fenster **Quelle für das Abbild wählen**.

Schritt 2. Quelle für das Abbild wählen

Wenn Sie im ersten Fenster des Assistenten das Kontrollkästchen **Vorhandenes Abbild verwenden**, aktiviert haben, wird dieser Schritt übersprungen.

Bei diesem Schritt muss aus folgenden Varianten eine Quelle für das Disk-Abbild ausgewählt werden:

- Wählen Sie die Variante **Abbild von lokaler Festplatte oder Netzlaufwerk kopieren**, wenn Sie über eine gespeicherte Notfall-CD verfügen oder auf Ihrem Computer bzw. in einer Ressource des lokalen Netzwerks ein Disk-Abbild (Datei im ISO-Format) bereitliegt.
- Wählen Sie die Variante **Abbild von Kaspersky-Lab-Server herunterladen**, wenn Sie nicht über eine Abbild-Datei für die Notfall-CD verfügen und die Abbild-Datei vom Kaspersky-Lab-Server herunterladen möchten (Dateigröße ca. 175 MB).

Schritt 3. Disk-Abbild kopieren (herunterladen)

Wenn Sie im ersten Fenster des Assistenten das Kontrollkästchen **Vorhandenes Abbild verwenden**, aktiviert haben, wird dieser Schritt übersprungen.

Wenn Sie beim vorherigen Schritt die Variante **Abbild von lokaler Festplatte oder Netzlaufwerk kopieren** ausgewählt haben, klicken Sie auf **Durchsuchen**. Nachdem Sie den Pfad zur Datei angegeben haben, klicken Sie auf **Weiter**. Im Assistentenfenster wird angezeigt, wie das Kopieren des Disk-Abbilds verläuft.

Wenn Sie beim vorherigen Schritt die Variante **Abbild von Kaspersky-Lab-Server herunterladen** ausgewählt haben, wird sofort der Download des Disk-Abbilds angezeigt.

Nach Abschluss des Kopiervorgangs oder des Ladens des Disk-Abbilds wechselt der Assistent automatisch zum nächsten Schritt.

Schritt 4. Abbild-Datei aktualisieren

Der Vorgang zur Aktualisierung der Abbild-Datei umfasst folgende Aktionen:

- Update der Antiviren-Datenbanken.
- Aktualisierung der Konfigurationsdateien.

Die Konfigurationsdateien definieren die Möglichkeit zum Hochfahren des Computers von einem Wechseldatenträger (beispielsweise von einer CD / DVD oder einem USB-Gerät mit der Notfall-CD), der mit dem Assistenten erstellt wurde.

Für die Aktualisierung der Antiviren-Datenbanken werden die beim letzten Update von Kaspersky Internet Security heruntergeladenen Datenbanken verwendet. Wenn die Datenbanken veraltet sind, wird empfohlen, die Updateaufgabe auszuführen und den Notfall-CD-Assistenten erneut zu starten.

Klicken Sie auf **Weiter**, um die Aktualisierung der Datei zu starten. Im Assistentenfenster wird angezeigt, wie die Aktualisierung verläuft.

Schritt 5. Disk-Abbild auf Datenträger schreiben

In diesem Fenster informiert der Assistent darüber, dass das Notfall-CD-Abbild erfolgreich erstellt wurde, und bietet Ihnen an, das Disk-Abbild auf einen Datenträger zu schreiben.

Geben Sie den Datenträger an, auf den die Notfall-CD geschrieben werden soll:

- Wählen Sie die Variante **Auf CD/DVD brennen** und geben Sie das Laufwerk an, auf das das Abbild geschrieben werden soll, um das Abbild auf eine CD / DVD zu brennen.
- Wählen Sie die Variante **Auf USB-Gerät schreiben** und geben Sie das Gerät an, auf das das Abbild geschrieben werden soll, um das Abbild auf ein USB-Gerät zu schreiben.

> Kaspersky Lab rät davon ab, Disk-Abbilder auf Geräten zu speichern, die nicht ausschließlich für die Datenspeicherung konzipiert sind, wie z.B. Smartphones, Mobiltelefone, PDAs und MP3-Player. Solche Geräte können bei Verwendung für die Speicherung von Disk-Abbildern in ihrer Funktion beeinträchtigt werden.

- Wählen Sie die Variante **Abbild in einer Datei auf lokaler Festplatte oder Netzlaufwerk speichern**, um das Abbild auf die Festplatte Ihres Computers oder auf einem anderen Computer zu schreiben, auf den Sie über das Netzwerk zugreifen können. Legen Sie dann den Ordner fest, in den das Disk-Abbild geschrieben werden soll, und geben Sie einen Namen für die Datei im ISO-Format an.

Schritt 6. Assistent abschließen

Klicken Sie auf **Beenden**, um die Arbeit des Assistenten abzuschließen. Sie können die erstellte Notfall-CD zum Booten des Computers (s. S. 61) verwenden, wenn es aufgrund von Viren- und Malware-Aktivitäten nicht mehr im normalen Modus möglich ist, den Computer hochzufahren und Kaspersky Internet Security zu starten.

HOCHFAHREN EINES COMPUTERS MIT HILFE DER NOTFALL-CD

Wenn sich das Betriebssystem aufgrund eines Virenangriffs nicht mehr hochfahren lässt, können Sie die Notfall-CD einsetzen.

Um das Betriebssystem zu booten, ist eine CD / DVD oder ein USB-Gerät erforderlich, auf der/dem das Programm Notfall-CD gespeichert ist (s. Abschnitt "Notfall-CD erstellen" auf S. 58).

Das Booten des Computers von einem Wechseldatenträger ist nicht immer möglich. Dies wird beispielsweise von einigen älteren Computermodellen nicht unterstützt. Klären Sie zuerst, ob diese Option möglich ist, bevor Sie den Computer herunterfahren, um ihn anschließend von einem Wechseldatenträger zu booten.

Gehen Sie folgendermaßen vor, um den Computer mit einer Notfall-CD zu booten:

1. Aktivieren Sie in den BIOS-Einstellungen das Booten von CD / DVD oder von USB-Gerät (Weitere Informationen finden Sie in der Dokumentation zum Motherboard Ihres Computers).

2. Legen Sie die CD / DVD mit dem Programm Notfall-CD in das Laufwerk des infizierten Computers ein oder schließen Sie das USB-Gerät mit dem Programm Notfall-CD an den Computer an.

3. Starten Sie den Computer neu.

Ausführliche Informationen über die Verwendung der Notfall-CD bietet das Benutzerhandbuch zur Kaspersky Notfall-CD, das Sie als PDF-Datei auf der Programm-CD oder unter www.kaspersky.de/downloads finden.

BERICHT ÜBER DIE PROGRAMMAKTIVITÄT ANZEIGEN

Kaspersky Internet Security führt Berichte über die Arbeit aller Komponenten. Der Bericht bietet statistische Informationen über das Programm (Sie können beispielsweise nachsehen, wieviele schädliche Objekte das Programm in einem bestimmten Zeitraum gefunden und neutralisiert hat, wie oft das Programm in diesem Zeitraum aktualisiert wurde, wie viele Spam-Mails gefunden wurden, u.a.).

Auf einem Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 können Sie mit Hilfe des Kaspersky Gadgets die Berichte öffnen. Dafür muss eine der Schaltflächen des Kaspersky Gadgets mit der Funktion zum Anhalten des Schutzes belegt sein (s. Abschnitt "Wie wird das Kaspersky Gadget verwendet?" auf S. 63).

Gehen Sie folgendermaßen vor, um einen Bericht über die Programmarbeit anzuzeigen:

1. Öffnen Sie das Fenster **Berichte**. Dafür gibt es unterschiedliche Möglichkeiten:

   - verwenden Sie im oberen Bereich des Programmhauptfensters den Link **Berichte**.

   - klicken Sie im Interface des Kaspersky Gadgets auf die Schaltfläche mit dem Symbol **Berichte** (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7).

   Im Fenster **Berichte** werden Berichte über die Programmarbeit als Diagramme dargestellt.

2. Klicken Sie unten im Fenster **Bericht** auf **Detaillierter Bericht**, um einen ausführlichen Bericht über die Arbeit des Programms zu öffnen (z.B. über die Arbeit der einzelnen Programmkomponenten).

   Das Fenster **Detaillierter Bericht** wird geöffnet. Hier werden die Daten in Tabellenform dargestellt. Die Berichtseinträge können auf unterschiedliche Weise angeordnet werden.

STANDARDEINSTELLUNGEN DES PROGRAMMS WIEDERHERSTELLEN

Sie können jederzeit die von Kaspersky Lab empfohlenen Einstellungen für Kaspersky Internet Security wiederherstellen. Die Wiederherstellung der Einstellungen erfolgt mit Hilfe des *Konfigurationsassistenten für das Programm*.

Der Assistent stellt für alle Schutzkomponenten die Sicherheitsstufe **Empfohlen** ein. Wenn die empfohlene Sicherheitsstufe wiederhergestellt wird, können Sie Einstellungsänderungen beibehalten, die zuvor für die Programmkomponenten angepasst wurden.

➧ *Gehen Sie folgendermaßen vor, um die standardmäßigen Programmeinstellungen wiederherzustellen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Starten Sie den Konfigurationsassistenten für das Programm mit einer der folgenden Methoden:
   - Klicken Sie im unteren Fensterbereich auf den Link **Wiederherstellen**.
   - Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Unterabschnitt **Programmkonfiguration** und klicken Sie im Block **Standardeinstellungen wiederherstellen** auf **Wiederherstellen**.

Details zu den einzelnen Schritten des Assistenten

Schritt 1. Assistent starten

Klicken Sie auf den Link **Weiter**, um den Assistenten fortzusetzen.

Schritt 2. Einstellungen wiederherstellen

Das Fenster enthält die Schutzkomponenten von Kaspersky Internet Security, deren Einstellungen vom Benutzer verändert oder von Kaspersky Internet Security beim Training der Komponenten Firewall und Anti-Spam gesammelt wurden. Wenn für eine bestimmte Komponente individuelle Einstellungen festgelegt wurden, werden diese ebenfalls in diesem Fenster genannt.

Als Einstellungen gelten: Erlaubnisliste und Verbotsliste mit Phrasen und Adressen für die Komponente Anti-Spam, Listen mit vertrauenswürdigen Internetadressen und Telefonnummern von Internetprovidern, Ausnahmeregeln für die Programmkomponenten, Firewall-Filterregeln für Pakete und Programme.

Die Einstellungen werden bei der Arbeit von Kaspersky Internet Security festgelegt. Dabei werden individuelle Aufgaben und Sicherheitsanforderungen berücksichtigt. Kaspersky Lab empfiehlt, die unikalen Einstellungen zu speichern, wenn die ursprünglichen Programmeinstellungen wiederhergestellt werden.

Aktivieren Sie die Kontrollkästchen für die Einstellungen, die gespeichert werden sollen, und klicken Sie auf **Weiter**.

Schritt 3. Systemanalyse

Auf dieser Etappe werden Informationen über Programme, die zu Microsoft Windows gehören, gesammelt. Diese Programme werden in die Liste der vertrauenswürdigen Anwendungen aufgenommen, deren Aktionen im System nicht beschränkt werden.

Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 4. Wiederherstellung abschließen

Klicken Sie auf **Beenden**, um die Arbeit des Assistenten abzuschließen.

WIE PROGRAMMEINSTELLUNGEN VON KASPERSKY INTERNET SECURITY AUF EINEN ANDEREN COMPUTER ÜBERTRAGEN WERDEN.

Sie können Ihre Programmeinstellungen für ein anderes Exemplar von Kaspersky Internet Security übernehmen, das auf einem anderen Computer installiert ist. Auf diese Weise sind die Einstellungen des Programms auf beiden Computern identisch. Diese Option kann beispielsweise von Nutzen sein, wenn Sie Kaspersky Internet Security auf Ihrem PC zuhause und im Büro installiert haben.

Die Programmeinstellungen werden in einer Konfigurationsdatei gespeichert, die Sie von Computer zu Computer übertragen können.

Die Übertragung der Einstellungen für Kaspersky Internet Security anderen umfasst drei Etappen:

1. Programmeinstellungen in einer Konfigurationsdatei speichern.
2. Konfigurationsdatei auf einen anderen Computer übertragen (beispielsweise per E-Mail oder auf einem Wechseldatenträger).
3. Einstellungen aus der Konfigurationsdatei in das Programm übernehmen, das auf dem anderen Computer installiert ist.

➨ *Gehen Sie folgendermaßen vor, um die aktuellen Einstellungen von Kaspersky Internet Security zu exportieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Einstellungen verwalten**.
3. Klicken Sie auf der rechten Fensterseite auf **Speichern**.
4. Geben Sie im folgenden Fenster einen Namen für die Konfigurationsdatei an und wählen Sie einen Speicherort dafür aus.
5. Klicken Sie auf **OK**.

➨ *Gehen Sie folgendermaßen vor, um die Funktionsparameter aus einer Konfigurationsdatei zu importieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Einstellungen verwalten**.
3. Klicken Sie auf der rechten Fensterseite auf **Laden**.
4. Wählen Sie im folgenden Fenster eine Datei aus, aus der Sie die Parameter für Kaspersky Internet Security importieren möchten.
5. Klicken Sie auf **OK**.

WIE DAS KASPERSKY GADGET VERWENDET WIRD.

Wenn Kaspersky Internet Security auf einem Computer mit Microsoft Windows Vista oder Microsoft Windows 7 eingesetzt wird, steht das Kaspersky Gadget zur Verfügung (weiter auch einfach als *Gadget* bezeichnet). Nach der Installation von Kaspersky Internet Security auf einem Computer mit Microsoft Windows 7 erscheint das Gadget automatisch auf dem Desktop. Wenn das Programm auf einem Computer mit dem Betriebssystem Microsoft Windows

Vista installiert wird, muss das Gadget manuell zur Sidebar von Microsoft Windows hinzugefügt werden (s. Dokumentation des Betriebssystems).

Der Farbindikator des Gadgets signalisiert den Schutzstatus Ihres Computers. Er entspricht dem Indikator im Programmhauptfenster (s. Abschnitt "Probleme im Computerschutz diagnostizieren und beheben" auf S. 42). Die Farbe Grün bedeutet, dass der Computer sicher ist. Gelb signalisiert, dass der Schutz Probleme aufweist, und Rot warnt vor einer ernsthaften Bedrohung für die Computersicherheit. Ist der Indikator grau, so wurde das Programm angehalten.

Während einer Aktualisierung der Datenbanken und Programm-Module erscheint in der Mitte des Gadgets ein rotierender Globus.

Mit Hilfe des Gadgets können Sie folgende Aktionen ausführen:

- Programm fortsetzen, nachdem es angehalten wurde.
- Programmhauptfenster öffnen
- einzelne Objekte auf Viren untersuchen
- News-Fenster öffnen

Außerdem können Sie die Gadget-Schaltflächen mit zusätzlichen Aktionen belegen:

- Update starten.
- Programmeinstellungen ändern.
- Programmberichte anzeigen.
- in die Sichere Umgebung wechseln (nur für 32-Bit-Betriebssysteme)
- Berichte über Kindersicherung anzeigen.
- Informationen zur Netzwerkaktivität (Netzwerkmonitor) und zur Programmaktivität anzeigen
- Schutz anhalten
- Virtuelle Tastatur öffnen
- Aufgabenübersicht öffnen

➡ *Um das Programm mit Hilfe des Gadgets zu starten,*

klicken Sie auf das Symbol ⏻ in der Mitte des Gadgets auf das Symbol **Aktivieren**.

➡ *Um das Programmhauptfenster mit Hilfe des Gadgets zu öffnen:*

klicken Sie in der Mitte des Gadgets auf das Monitorsymbol.

➡ *Um ein Objekt mit Hilfe des Gadgets auf Viren zu untersuchen,*

ziehen Sie das Untersuchungsobjekt auf das Gadget.

Der Fortschritt der Aufgabenausführung wird im Fenster **Aufgabenübersicht** dargestellt.

➡ *Um mit Hilfe des Gadgets das Fenster zur Anzeige der Neuigkeiten zu öffnen:*

klicken Sie auf das Symbol ✉, das in der Mitte des Gadgets angezeigt wird, wenn Neuigkeiten erschienen sind.

Gehen Sie folgendermaßen vor, um das Gadget anzupassen:

1. Öffnen Sie das Gadget-Konfigurationsfenster durch Klick auf das Symbol , das rechts oben im Gadget-Block erscheint, wenn mit der Maus darauf gezeigt wird.
2. Wählen Sie in den Dropdown-Listen, die den Gadget-Schaltflächen entsprechen, die Aktionen, die bei Klick auf die Gadget-Schaltfläche ausgeführt werden sollen.
3. Klicken Sie auf **OK**.

REPUTATION EINES PROGRAMMS ÜBERPRÜFEN

Kaspersky Internet Security ermöglicht es, die Reputation von Programmen zu ermitteln. Dazu dienen Daten, die von Benutzern aus der ganzen Welt stammen. Die Reputation eines Programms umfasst folgende Kriterien:

- Name des Herstellers
- Informationen zur digitalen Signatur (verfügbar, wenn eine digitale Signatur vorhanden ist).
- Informationen zur Gruppe, in die ein Programm von der Programmkontrolle oder von der Mehrheit der Benutzer des Kaspersky Security Network eingeordnet wurde.
- Anzahl der Benutzer von Kaspersky Security Network, die ein Programm verwenden (verfügbar, wenn das Programm in der Datenbank des Kaspersky Security Network zur Gruppe Vertrauenswürdig gehört).
- Zeitraum, seit dem das Programm im Kaspersky Security Network bekannt ist.
- Länder, in denen ein Programm am häufigsten vorkommt.

Um die Reputation eines Programms zu überprüfen, müssen Sie bei der Installation von Kaspersky Internet Security der Teilnahme am Kaspersky Security Network (s. S. 185) zustimmen.

Um die Reputation eines Programms zu ermitteln,

öffnen Sie das Kontextmenü der ausführbaren Programmdatei und wählen Sie den Punkt **Reputation im KSN nachsehen**.

SIEHE AUCH

ERWEITERTE PROGRAMMEINSTELLUNGEN

Dieser Abschnitt informiert darüber, wie die einzelnen Programmkomponenten angepasst werden.

IN DIESEM ABSCHNITT

GRUNDLEGENDE SCHUTZPARAMETER

Im Fenster mit den Programmeinstellungen können Sie unter **Allgemeine Einstellungen** im Abschnitt **Schutz-Center** die folgenden Operationen ausführen:

- alle Schutzkomponenten deaktivieren (s. Abschnitt "Schutz aktivieren und deaktivieren" auf S. 43);
- automatischen oder interaktiven Schutzmodus auswählen (s. Abschnitt"Schutzmodus auswählen" auf S. 68);
- Zugriff der Benutzer auf das Programm mittels Kennwort beschränken (s. Abschnitt "Kontrolle des Zugriffs auf Kaspersky Internet Security" auf S. 67);
- automatischen Programmstart bei Hochfahren des Betriebssystems aktivieren oder deaktivieren (s. Abschnitt "Automatischen Start aktivieren und deaktivieren" auf S. 41);
- festgelegte Tastenkombination zur Anzeige der virtuellen Tastatur auf dem Bildschirm aktivieren (s. Abschnitt "Schutz vor dem Abfangen von Tastatureingaben" auf S. 53).

IN DIESEM ABSCHNITT

KONTROLLE DES ZUGRIFFS AUF KASPERSKY INTERNET SECURITY.

Es kann sein, dass ein PC von mehreren Benutzern verwendet wird, deren Fertigkeiten im Umgang mit Computern völlig unterschiedlich sind. Der uneingeschränkte Zugriff der Benutzer auf Kaspersky Internet Security und dessen Einstellungen kann das Sicherheitsniveau des Computers stark beeinträchtigen.

Um den Zugriff auf das Programm zu beschränken, können Sie ein Kennwort festlegen und angeben, für welche Aktionen dieses abgefragt werden soll:

- Programmeinstellungen ändern
- Kindersicherung aktivieren und anpassen
- Programm beenden
- Programm deinstallieren

Bewahren Sie das Kennwort für die Beschränkung der Programmdeinstallation sicher auf. Wenn Sie das Kennwort vergessen sollten, wird es schwierig sein, das Programm vom Computer zu entfernen.

➡ *Gehen Sie folgendermaßen vor, um den Zugriff auf Kaspersky Internet Security durch ein Kennwort zu beschränken:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Allgemeine Einstellungen**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Kennwortschutz** das Kontrollkästchen **Kennwortschutz aktivieren** und klicken Sie auf **Einstellungen**.
4. Geben Sie im folgenden Fenster **Kennwortschutz** das Kennwort an und legen Sie den Bereich fest, für den die Zugriffsbeschränkung gelten soll.

SCHUTZMODUS WÄHLEN

Kaspersky Internet Security arbeitet standardmäßig im *automatischen Schutzmodus*. In diesem Modus wendet das Programm beim Auftreten gefährlicher Ereignisse automatisch die von Kaspersky Lab empfohlene Aktion an. Sie können den *interaktiven Schutzmodus* wählen, damit Kaspersky Internet Security Sie über alle gefährlichen und verdächtigen Ereignisse im System informiert und Ihnen das Programm mögliche Aktionen zur Auswahl anbietet.

➧ *Gehen Sie folgendermaßen vor, um einen Schutzmodus zu wählen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** den Abschnitt **Allgemeine Einstellungen**.
3. Deaktivieren oder aktivieren Sie im Block **Interaktiver Modus** die Kontrollkästchen für den entsprechenden Schutzmodus:
   - um den interaktiven Schutzmodus zu wählen, deaktivieren Sie das Kontrollkästchen **Aktion automatisch wählen**.
   - um den automatischen Schutzmodus zu wählen, aktivieren Sie das Kontrollkästchen **Aktion automatisch wählen**.

     Damit verdächtige Objekte bei der Arbeit im automatischen Modus nicht gelöscht werden, aktivieren Sie das Kontrollkästchen **Verdächtige Objekte nicht löschen**.

UNTERSUCHUNG DES COMPUTERS

Die Untersuchung des Computers auf Schwachstellen, Viren und andere bedrohliche Programme ist eine der wichtigsten Aufgaben für die Sicherheit des Rechners.

Ihr Computer muss regelmäßig auf Viren und andere bedrohliche Programme überprüft werden, um auszuschließen, dass sich schädliche Programm ausbreiten, die nicht von den Schutzkomponenten erkannt wurden, da beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Die Aufgabe zur Schwachstellensuche umfasst eine Sicherheitsdiagnose des Betriebssystems und eine Software-Analyse zum Erkennen von Sicherheitslücken, die Angreifern zur Verbreitung schädlicher Objekte und zum Zugriff auf persönliche Daten dienen können.

Dieser Abschnitt informiert über Besonderheiten und Konfiguration von Untersuchungsaufgaben sowie über Sicherheitsstufen, Methoden und Technologien für die Untersuchung.

IN DIESEM ABSCHNITT

VIRENSUCHE

Kaspersky Internet Security verfügt über folgende Aufgaben zur Suche nach Viren und anderen bedrohlichen Programmen:

- **Vollständige Untersuchung**. Untersuchung des gesamten Systems. Standardmäßig untersucht Kaspersky Internet Security folgende Objekte:

- Systemspeicher
- Objekte, die beim Hochfahren des Betriebssystems geladen werden.
- Systemsicherung
- Mail-Datenbanken
- Festplatten, Wechseldatenträger und Netzlaufwerke

- **Untersuchung wichtiger Bereiche**. Standardmäßig untersucht Kaspersky Internet Security die Objekte, die beim Hochfahren des Betriebssystems geladen werden.
- **Benutzerdefinierte Untersuchung**. Kaspersky Internet Security untersucht die vom Benutzer ausgewählten Objekte. Sie können ein beliebiges Objekt aus der folgenden Liste untersuchen:
  - Systemspeicher
  - Objekte, die beim Hochfahren des Betriebssystems geladen werden.
  - Systemsicherung
  - Mail-Datenbanken
  - Festplatten, Wechseldatenträger und Netzlaufwerke
  - eine beliebige Datei oder einen Ordner

Bei den Aufgaben zur vollständigen Untersuchung und zur Untersuchung wichtiger Bereiche handelt es sich um spezifische Aufgaben. Es wird davor gewarnt, die Liste der Untersuchungsobjekte für diese Aufgaben zu ändern.

Jede Untersuchungsaufgabe wird in einem bestimmten Bereich ausgeführt und kann nach einem festgelegten Zeitplan gestartet werden. Außerdem wird jede Untersuchungsaufgabe durch eine Sicherheitsstufe charakterisiert (Auswahl von Einstellungen für die Genauigkeit der Untersuchung). In der Grundeinstellung ist immer der *Signaturmodus* aktiviert. Dabei werden zur Virensuche die Einträge der Programm-Datenbanken verwendet. Außerdem können Sie verschiedene Methoden und Technologien zur Untersuchung einsetzen.

Nach dem Start einer Aufgabe zur vollständigen Untersuchung oder zur Untersuchung wichtiger Bereiche wird der Fortschritt im Fenster **Untersuchung** unter der laufenden Aufgabe sowie in der Aufgabenübersicht angezeigt (s. Abschnitt "Untersuchungsaufgaben verwalten. Aufgabenübersicht" auf S. 76).

Beim Fund einer Bedrohung weist Kaspersky Internet Security dem gefundenen Objekt eine der folgenden Statusvarianten zu:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- Status *möglicherweise infiziert* (verdächtig) wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise enthält die Datei eine virentypische Codefolge oder den modifizierten Code eines bekannten Virus.

Anschließend zeigt das Programm eine Meldung (s. S. 182) über die gefundene Bedrohung an und führt die festgelegte Aktion aus. Sie können die Aktion beim Fund einer Bedrohung ändern.

Wenn Sie im automatischen Modus (s. Abschnitt "Schutzmodus auswählen" auf S. 68) arbeiten, führt Kaspersky Internet Security beim Fund gefährlicher Objekte automatisch die von den Kaspersky-Lab-Experten empfohlenen Aktionen aus. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige – **In die Quarantäne verschieben**. Wenn Sie im interaktiven Modus arbeiten (s. Abschnitt "Schutzmodus auswählen" auf S. 68), zeigt das Programm beim Fund gefährlicher Objekte eine Meldung an, in der Sie die erforderliche Aktion auswählen können.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren. Verdächtige (möglicherweise infizierte) Objekte werden in die Quarantäne verschoben. Sie können eine automatische Untersuchung der Quarantänedateien nach jedem Update festlegen.

Informationen über die Untersuchungsergebnisse und über alle Ereignisse, die bei der Aufgabenausführung auftreten, werden im Bericht von Kaspersky Internet Security (s. S. 177) protokolliert.

IN DIESEM ABSCHNITT

SICHERHEITSSTUFE ÄNDERN UND WIEDERHERSTELLEN

Sie können eine vordefinierte Sicherheitsstufe wählen, die Ihren Anforderungen entspricht, oder die Untersuchungseinstellungen entsprechend anpassen.

Während Sie eine Untersuchungsaufgabe anpassen, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese Einstellungen gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und entsprechen der Sicherheitsstufe **Empfohlen**.

Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**).
3. Stellen Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

> Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die empfohlenen Untersuchungseinstellungen wiederherzustellen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**).

3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Standard**.

ZEITPLAN FÜR DEN UNTERSUCHUNGSSTART ERSTELLEN

Es kann ein Zeitplan für den automatischen Start einer Untersuchungsaufgabe angelegt werden: In diesem werden eine Frequenz für den Aufgabenstart, ein Startzeitpunkt (falls erforderlich) sowie zusätzliche Einstellungen festgelegt.

Wenn der Start aus irgendeinem Grund nicht möglich war (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet war), können Sie festlegen, dass der Start einer übersprungenen Aufgabe automatisch zum nächstmöglichen Zeitpunkt erfolgt. Außerdem lässt sich festlegen, dass eine Untersuchung automatisch angehalten wird, wenn der Bildschirmschoner inaktiv oder der Computer entsperrt ist. Diese Option erlaubt es, den Start einer Aufgabe zurückzustellen, bis der Benutzer seine Arbeit auf dem Computer beendet hat. Dadurch wird verhindert, dass eine Untersuchungsaufgabe Computerressourcen verbraucht, während diese für andere Aufgaben benötigt werden.

Der spezielle Modus zur Untersuchung im Computerleerlauf (s. Abschnitt "Aufgabenstart im Hintergrundmodus" auf S. 166) erlaubt es, eine Untersuchung des Arbeitsspeichers, der Systempartition und der Autostart-Objekte dann zu starten, wenn der Computer nicht verwendet wird.

➡ *Gehen Sie folgendermaßen vor, um den Startzeitplan einer Untersuchungsaufgabe anzupassen:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Schwachstellensuche**).

3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus, wählen Sie die gewünschten Werte für die Einstellung **Frequenz** aus und konfigurieren Sie den Startmodus für die Untersuchung.

➡ *Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Schwachstellensuche**).

3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus und aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.

➡ *Gehen Sie folgendermaßen vor, damit die Untersuchung erst gestartet wird, nachdem der Benutzer seine Arbeit beendet hat:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Schwachstellensuche**).

3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** und aktivieren Sie das Kontrollkästchen **Geplante Untersuchung ausführen, wenn Computer gesperrt ist oder Bildschirmschoner aktiviert wurde**.

LISTE DER UNTERSUCHUNGSOBJEKTE ERSTELLEN

Standardmäßig entspricht jeder Aufgabe zur Virensuche eine eigene Liste von Objekten. Zu diesen Objekten können sowohl Objekte des Computerdateisystems (z.B. logische Laufwerke, Mail-Datenbanken), als auch Objekte anderer Typen (z.B. Netzlaufwerke) gehören. Diese Liste kann geändert werden.

Wenn der Untersuchungsbereich leer ist oder kein Objekt des Untersuchungsbereichs angekreuzt wurde, kann die Untersuchungsaufgabe nicht gestartet werden.

Gehen Sie folgendermaßen vor, um für eine Aufgabe zur benutzerdefinierten Untersuchung eine Liste mit Untersuchungsobjekten zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Untersuchung**.
3. Öffnen Sie im unteren Fensterbereich mit dem Link **auswählen** die Liste der Untersuchungsobjekte.
4. Klicken Sie im folgenden Fenster **Benutzerdefinierte Untersuchung** auf **Hinzufügen**.
5. Wählen Sie im folgenden Fenster **Untersuchungsobjekt wählen ein Objekt** aus und klicken Sie auf **Hinzufügen**. Nachdem alle erforderlichen Objekte hinzugefügt wurden, klicken Sie auf **OK**. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie die entsprechenden Kontrollkästchen.

   Dateien, die gescannt werden sollen, können auch direkt in einen speziell markierten Bereich im Abschnitt **Untersuchung** gezogen werden.

Gehen Sie folgendermaßen vor, um für die Aufgaben zur vollständigen Untersuchung, zur Untersuchung wichtiger Bereiche und zur Schwachstellensuche eine Liste mit Untersuchungsobjekten zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Untersuchungsaufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Schwachstellensuche**).
3. Klicken Sie auf der rechten Fensterseite auf **Untersuchungsobjekte**.
4. Erstellen Sie im folgenden Fenster **Untersuchungsobjekte** mit Hilfe der Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** eine Liste. Um bestimmte Objekte aus der Untersuchungsliste auszuschließen, deaktivieren Sie die entsprechenden Kontrollkästchen.

   Objekte, die sich standardmäßig in der Liste befinden, können nicht geändert oder gelöscht werden.

UNTERSUCHUNGSMETHODEN WÄHLEN

Bei einer Virenuntersuchung des Computers wird immer die Methode *Signaturanalyse* verwendet, bei der Kaspersky Internet Security ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht.

Um die Effektivität der Suche zu steigern, stehen zusätzliche Untersuchungsmethoden zur Verfügung: *heuristische Analyse* (Analyse der Aktivität, die ein Objekt im System zeigt) und *Rootkit-Suche* (Utilities, die schädliche Programme im Betriebssystem verstecken).

Gehen Sie folgendermaßen vor, um die erforderlichen Untersuchungsmethoden zu wählen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**).

3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Wählen Sie auf der Registerkarte **Erweitert** im Block **Untersuchungsmethoden** die erforderlichen Untersuchungsmethoden aus.

UNTERSUCHUNGSTECHNOLOGIEN WÄHLEN

Neben den Untersuchungsmethoden können Sie für die Objektuntersuchung spezielle Technologien einsetzen, mit denen die Untersuchung beschleunigt werden kann. Dabei werden Dateien ausgeschlossen, die seit dem letzten Scan nicht verändert wurden.

➡ *Gehen Sie folgendermaßen vor, um die Technologien zur Objektuntersuchung zu wählen:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**).

3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** die gewünschten Werte.

AKTION BEIM FUND EINER BEDROHUNG ÄNDERN

Beim Fund von infizierten Objekten führt das Programm eine festgelegte Aktion aus.

➡ *Gehen Sie folgendermaßen vor, um die beim Fund einer Bedrohung auszuführende Aktion zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**).

3. Wählen Sie auf der rechten Fensterseite im Block **Aktion beim Fund einer Bedrohung** die entsprechende Option aus.

UNTERSUCHUNGSSTART MIT DEN RECHTEN EINES ANDEREN BENUTZERS

Die Untersuchungsaufgaben werden standardmäßig unter dem Benutzerkonto gestartet, mit dessen Rechten Sie sich im System angemeldet haben. Es kann aber erforderlich sein, eine Aufgabe mit den Rechten eines anderen Benutzers zu starten. Sie können das Benutzerkonto festlegen, mit dessen Rechten eine Untersuchungsaufgabe gestartet werden soll.

➡ *Gehen Sie folgendermaßen vor, um die Untersuchung mit den Rechten eines anderen Benutzers zu starten:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Schwachstellensuche**).

3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen **Aufgabe starten mit Rechten des Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

TYP DER ZU UNTERSUCHENDEN OBJEKTE ÄNDERN

Durch die Angabe des Typs der zu untersuchenden Objekte bestimmen Sie das Format der Dateien, die beim Ausführen der gewählten Aufgabe untersucht werden sollen.

Bei der Auswahl des Dateityps muss Folgendes beachtet werden:

- Es gibt eine Reihe von Dateiformaten (z.B. TXT), für die das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung relativ gering ist. Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (EXE, DLL, DOC). Das Risiko, dass schädlicher Code in solche Dateien eindringt und aktiviert wird, ist relativ hoch.
- Ein Angreifer kann einen Virus in einer ausführbaren Datei, die in eine txt-Datei umbenannt wurde, an Ihren Computer senden. Wenn Sie die Untersuchung von Dateien nach Erweiterung gewählt haben, wird eine solche Datei bei der Untersuchung übersprungen. Wurde die Untersuchung von Dateien nach Format gewählt, ignoriert Datei-Anti-Virus die Erweiterung und analysiert die Kopfzeile der Datei, wodurch sich ergeben kann, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Gehen Sie folgendermaßen vor, um den Typ der zu untersuchenden Dateien zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**).
3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Dateitypen** die gewünschte Variante.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie beispielsweise Archive, Installationspakete, angehängte OLE-Objekte und Dateien in Mailformaten. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Für jeden Typ einer zusammengesetzten Datei können Sie wählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie zur Auswahl den Link neben dem Namen des Objekts. Er verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn der Modus gewählt wurde, in dem nur neue und veränderte Dateien untersucht werden (s. S. 75), stehen die Links zur Auswahl aller oder nur neuer Dateien nicht zur Verfügung.

Außerdem können Sie festlegen, bis zu welcher maximalen Größe eine zusammengesetzte Datei untersucht werden soll. Zusammengesetzte Dateien, die den festgelegten Wert überschreiten, werden nicht untersucht.

Wenn umfangreiche Dateien aus Archiven extrahiert werden, erfolgt eine Untersuchung auch dann, wenn das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.

Gehen Sie folgendermaßen vor, um die Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**).
3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung von zusammengesetzten Dateien** die Typen der zusammengesetzten Dateien, die untersucht werden sollen.

Gehen Sie folgendermaßen vor, um eine maximale Größe für zusammengesetzte Dateien festzulegen, die untersucht werden sollen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**).
3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.
5. Aktivieren Sie im folgenden Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken und legen Sie die maximale Größe für zu untersuchende Dateien fest**.

UNTERSUCHUNG OPTIMIEREN

Sie können die Untersuchungsdauer verkürzen und die Arbeitsgeschwindigkeit von Kaspersky Internet Security erhöhen. Dies lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Außerdem kann die Untersuchungsdauer für ein einzelnes Objekt beschränkt werden. Wenn eine Datei nicht innerhalb der vorgegebenen Zeit untersucht wurde, wird sie von der laufenden Untersuchung ausgeschlossen (außer Archiven und Dateien, die aus mehreren Objekten bestehen).

Gehen Sie folgendermaßen vor, damit nur neue und veränderte Dateien untersucht werden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**).
3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung optimieren** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

Gehen Sie folgendermaßen vor, um die Untersuchungsdauer einzuschränken:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Untersuchung des Computers** die erforderliche Aufgabe (**Vollständige Untersuchung**, **Untersuchung wichtiger Bereiche** oder **Benutzerdefinierte Untersuchung**).
3. Klicken Sie für die gewählte Aufgabe im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Gültigkeitsbereich** im Block **Untersuchung optimieren** das Kontrollkästchen **Objekte überspringen, wenn Untersuchung länger andauert als** und geben Sie die Untersuchungsdauer für eine einzelne Datei an.

WECHSELDATENTRÄGER BEIM ANSCHLIEßEN UNTERSUCHEN

In letzter Zeit treten vermehrt schädliche Objekte auf, die Schwachstellen des Betriebssystems ausnutzen, um sich über lokale Netzwerke und Wechseldatenträger auszubreiten. Kaspersky Internet Security bietet eine Funktion, mit der Wechseldatenträger untersucht werden können, wenn sie an den Computer angeschlossen werden.

Gehen Sie folgendermaßen vor, um die Funktion anzupassen, mit der Wechseldatenträger untersucht werden, wenn sie an den Computer angeschlossen werden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Untersuchung des Computers** den Abschnitt **Allgemeine Einstellungen**.
3. Wählen Sie im Block **Wechseldatenträger beim Anschließen untersuchen** eine Aktion und begrenzen Sie bei Bedarf im Feld unten die Größe der zu untersuchenden Laufwerke.

VERKNÜPFUNG FÜR DEN AUFGABENSTART ERSTELLEN

Für den Schnellstart der Aufgaben zur vollständigen und schnellen Untersuchung sowie zur Schwachstellensuche ist im Programm die Möglichkeit vorgesehen, Verknüpfungen anzulegen. So kann die erforderliche Untersuchungsaufgabe gestartet werden, ohne das Programmhauptfenster oder das Kontextmenü zu öffnen.

Gehen Sie folgendermaßen vor, um eine Verknüpfung für den Start einer Untersuchungsaufgabe zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Untersuchung des Computers** den Abschnitt **Allgemeine Einstellungen**.
3. Klicken Sie auf der rechten Seite des Fensters im Block **Schneller Aufgabenstart** neben dem entsprechenden Aufgabennamen (**Untersuchung wichtiger Bereiche**, **Vollständige Untersuchung** oder **Schwachstellensuche**) auf **Verknüpfung erstellen**.
4. Geben Sie im folgenden Fenster an, wo und unter welchem Namen die Verknüpfung gespeichert werden soll. Standardmäßig wird die Verknüpfung unter dem Aufgabennamen im Ordner Arbeitsplatz des aktiven Computerbenutzers erstellt.

SUCHE NACH SCHWACHSTELLEN

Schwachstellen in einem Betriebssystem können beispielsweise auf Programmierfehler, unsichere Kennwörter oder Malware-Aktionen zurückgehen. Die Schwachstellensuche umfasst verschiedene Sicherheitsmaßnahmen wie beispielsweise Systemanalyse, Analyse der Einstellungen des Betriebssystems und des Browsers, und die Suche nach unsicheren Diensten.

Die Diagnose kann eine gewisse Zeit beanspruchen. Anschließend werden die gefundenen Probleme im Hinblick auf ihre Gefährlichkeit für das System analysiert.

Nach dem Start einer Aufgabe zur Schwachstellensuche (s. S. 51) wird der Fortschritt im Fenster **Untersuchung** unter **Schwachstellensuche** sowie in der Aufgabenübersicht angezeigt (s. Abschnitt "Untersuchungsaufgaben verwalten. Aufgabenübersicht" auf S. 76).

Informationen über die Ausführungsergebnisse einer Aufgabe zur Schwachstellensuche werden im Bericht für Kaspersky Internet Security (s. S. 177) protokolliert.

Wie für die Untersuchungsaufgaben kann auch für die Aufgabe zur Schwachstellensuche ein Startzeitplan erstellt, eine Liste der Untersuchungsobjekte angelegt (s. S. 72), ein Benutzerkonto gewählt (s. Abschnitt "Untersuchungsstart mit den Rechten eines anderen Benutzers" auf S. 73) und eine Verknüpfung für den schnellen Aufgabenstart erstellt werden. In der Grundeinstellung sind die auf dem Computer installierten Anwendungen als Untersuchungsobjekt gewählt.

UNTERSUCHUNGSAUFGABEN VERWALTEN. AUFGABENÜBERSICHT

In der Aufgabenübersicht werden Informationen über die letzten ausgeführten oder auszuführenden Aufgaben zur Computeruntersuchung angezeigt (z.B. Virensuche, Schwachstellensuche, Rootkit-Suche, Aktive Desinfektion).

Mithilfe der Aufgabenübersicht können Sie den Fortschritt und das Ergebnis einer Aufgabe anzeigen lassen oder die Aufgabe anhalten. Außerdem sind für einige Aufgaben zusätzliche Optionen verfügbar (Nach Abschluss der Schwachstellensuche können Sie beispielsweise die Liste der gefundenen Schwachstellen öffnen und die Schwachstellen beseitigen.).

Gehen Sie folgendermaßen vor, um die Aufgabenübersicht zu öffnen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Untersuchung**.
3. Klicken Sie im folgenden Fenster **Untersuchung** auf die Schaltfläche **Aufgabenübersicht**, die sich im rechten oberen Ecke des Fensters befindet.

UPDATE

Das Update der Datenbanken und Programm-Module von Kaspersky Internet Security gewährleistet den aktuellen Zustand Ihres Computerschutzes. Jeden Tag tauchen neue Viren, trojanische Programme und andere Malware auf. Informationen über Bedrohungen und entsprechende Neutralisierungsmethoden sind in den Datenbanken von Kaspersky Internet Security enthalten. Die Datenbanken und Programm-Module müssen regelmäßig aktualisiert werden, damit neue Bedrohungen rechtzeitig erkannt werden können.

Für ein regelmäßiges Update ist eine gültige Programmlizenz erforderlich. Ohne Lizenz können Sie das Programm nur ein Mal aktualisieren.

Bei einer Aktualisierung des Programms werden folgende Elemente auf Ihren Computer heruntergeladen und darauf installiert:

- Datenbanken für Kaspersky Internet Security.

  Der Schutz der Informationen auf ihrem Computer basiert auf Datenbanken, die Bedrohungssignaturen, Beschreibungen von Netzwerkangriffen sowie Informationen über entsprechende Desinfektionsmethoden enthalten. Die Schutzkomponenten verwenden diese Informationen bei der Suche nach und bei der Desinfektion von gefährlichen Objekten auf Ihrem Computer. Die Datenbanken werden regelmäßig durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird ausdrücklich empfohlen, die Datenbanken regelmäßig zu aktualisieren.

  Gemeinsam mit den Datenbanken von Kaspersky Internet Security werden auch die Netzwerktreiber aktualisiert, die die Funktionalität für das Abfangen des Netzwerkverkehrs durch die Schutzkomponenten gewährleisten.

- Programm-Module.

  Neben den Datenbanken von Kaspersky Internet Security können auch die Programm-Module aktualisiert werden. Updates für Programm-Module beheben Schwachstellen von Kaspersky Internet Security, fügen neue Funktionen hinzu und optimieren bestehende Funktionen.

Bei der Aktualisierung werden die auf Ihrem Computer installierten Programm-Module und Datenbanken mit der aktuellen Version verglichen, die in der Updatequelle vorliegt. Wenn die Datenbanken und Programm-Module nicht aktuell sind, werden fehlende Teile der Updates auf dem Computer installiert.

Wenn die Datenbanken stark veraltet sind, kann das Updatepaket relativ umfangreich sein und zusätzlichen Internet-Datenverkehr verursachen (bis zu mehreren Dutzend Megabyte).

Bevor die Datenbanken aktualisiert werden, legt Kaspersky Internet Security eine Sicherungskopie an. So können Sie bei Bedarf zur vorhergehenden Version der Datenbanken zurückkehren (s. Abschnitt "Rollback zum vorherigen Update" auf S. 80).

Informationen über den aktuellen Status der Datenbanken von Kaspersky Internet Security werden im Abschnitt **Update** des Programmhauptfensters angezeigt.

Informationen über die Update-Ergebnisse und über alle Ereignisse, die bei der Ausführung einer Updateaufgabe auftreten, werden im Bericht von Kaspersky Internet Security (s. S. 177) protokolliert.

Sie können eine Updatequelle auswählen (s. Abschnitt "Updatequelle auswählen" auf S. 78) und den automatischen Updatestart anpassen.

IN DIESEM ABSCHNITT

UPDATEQUELLE AUSWÄHLEN

Eine *Updatequelle* ist eine Ressource, die Updates für die Datenbanken und Programm-Module von Kaspersky Internet Security enthält.

Als primäre Updatequelle dienen die Kaspersky-Lab-Updateserver, auf denen Updates der Datenbanken und Programm-Module für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.

Um Updates erfolgreich von den Servern herunterzuladen, muss Ihr Computer mit dem Internet verbunden sein. In der Grundeinstellung wird die Internetverbindung automatisch ermittelt. Wenn Sie einen Proxyserver verwenden, kann es notwendig sein, die Parameter der Verbindung anzupassen (s. Abschnitt "Proxyserver-Einstellungen" auf S. 125).

Parallel zur Aktualisierung von Kaspersky Internet Security können Sie die Updates für Datenbanken und Programm-Module, die von den Kaspersky-Lab-Servern heruntergeladen werden, in einen lokalen Ordner (s. Abschnitt "Update aus dem gemeinsamen Ordner" auf S. 79) kopieren, auf den dann andere Netzwerkcomputer zugreifen können. Dadurch lässt sich Internet-Traffic einsparen.

UPDATE-QUELLE HINZUFÜGEN

In der Grundeinstellung enthält die Liste nur die Kaspersky-Lab-Updateserver. Sie können als Update-Quelle einen lokalen Ordner oder einen anderen Server hinzufügen. Wenn mehrere Ressourcen als Updatequellen gewählt wurden, greift Kaspersky Internet Security bei der Aktualisierung nach der Reihenfolge der Liste darauf zu und lädt die Updates von der ersten verfügbaren Quelle herunter.

➡ *Gehen Sie folgendermaßen vor, um eine Updatequelle hinzuzufügen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Update-Einstellungen**.
3. Klicken Sie auf der rechten Fensterseite auf **Updatequelle**.
4. Öffnen Sie im folgenden Fenster auf der Registerkarte **Quelle** das Auswahlfenster. Klicken Sie dazu auf die Schaltfläche **Hinzufügen**.
5. Wählen Sie im folgenden Fenster **Updatequelle wählen** den Ordner, der die Updates enthält, oder geben Sie im Feld **Quelle** die Adresse des Servers ein, von dem die Updates heruntergeladen werden sollen.

REGION DES UPDATESERVERS WÄHLEN

Wenn Sie die Kaspersky-Lab-Server als Updatequelle verwenden, kann der für Sie günstigste Serverstandort für den Update-Download gewählt werden. Kaspersky Lab verfügt in mehreren Ländern der Erde über Server.

Durch die Verwendung des geografisch am nächsten gelegenen Kaspersky-Lab-Updateservers kann sich die Dauer des Update-Downloads verkürzen und das Übertragungstempo erhöhen. In der Grundeinstellung werden Informationen über den aktuellen Standort aus der Registrierung des Betriebssystems verwendet. Sie können die Region jedoch auch manuell wählen.

➡ *Gehen Sie folgendermaßen vor, um die Region des Servers zu wählen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Update-Einstellungen**.
3. Klicken Sie auf der rechten Fensterseite auf **Updatequelle**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Quelle** im Block **Regionale Einstellungen** die Variante **Aus der Liste wählen** und wählen Sie aus der Dropdown-Liste das Land, in dem Sie sich gegenwärtig aufhalten.

UPDATE AUS DEM GEMEINSAMEN ORDNER

Um Internet-Datenverkehr einzusparen, kann festgelegt werden, dass Kaspersky Internet Security auf den Netzwerkcomputern aus einem gemeinsamen Ordner aktualisiert werden soll. In diesem Fall lädt ein Computer des Netzwerks das Updatepaket von den Kaspersky-Lab-Servern im Internet oder von einer anderen Webressource, auf der sich die aktuellen Updates befinden, herunter. Die heruntergeladenen Updates werden in einem gemeinsamen Ordner abgelegt, auf den die anderen Netzwerkcomputer zugreifen, um die Updates für Kaspersky Internet Security zu erhalten.

Wenn auf dem Betriebssystem Microsoft Windows 7 unter dem Benutzerkonto "Gast" gearbeitet wird, werden die Updates nicht in den gemeinsamen Ordner kopiert. Es wird empfohlen, sich mit einem anderen Benutzerkonto anzumelden, damit die Update-Verteilung möglich ist.

➡ *Gehen Sie folgendermaßen vor, um den Modus für die Update-Verteilung zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Update-Einstellungen**.
3. Aktivieren Sie im Block **Erweitert** das Kontrollkästchen **Updates in folgenden Ordner kopieren** und geben Sie darunter im Feld den Pfad des gemeinsamen Ordners an, in dem heruntergeladene Updates abgelegt werden sollen. Außerdem kann mit Hilfe der Schaltfläche **Durchsuchen** ein Ordner gewählt werden.

➡ *Gehen Sie folgendermaßen vor, damit Updates für den Computer aus einem gemeinsamen Ordner geladen werden:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Update-Einstellungen**.
3. Klicken Sie auf der rechten Fensterseite auf **Updatequelle**.
4. Öffnen Sie im folgenden Fenster auf der Registerkarte **Quelle** das Auswahlfenster. Klicken Sie dazu auf die Schaltfläche **Hinzufügen**.
5. Wählen Sie im folgenden Fenster **Updatequelle wählen** einen Ordner oder geben im Feld **Quelle** den vollständigen Pfad an.
6. Deaktivieren Sie auf der Registerkarte **Quelle** das Kontrollkästchen **Kaspersky-Lab-Updateserver**.

ZEITPLAN FÜR UPDATESTART ERSTELLEN

Es kann ein Zeitplan für den automatischen Start einer Updateaufgabe angelegt werden: In diesem werden eine Frequenz für den Aufgabenstart, ein Startzeitpunkt (falls erforderlich) sowie zusätzliche Einstellungen festgelegt.

Wenn der Start aus irgendeinem Grund nicht möglich war (wenn beispielsweise der Computer im betreffenden Moment ausgeschaltet war), können Sie festlegen, dass der Start einer übersprungenen Aufgabe automatisch zum nächstmöglichen Zeitpunkt erfolgt.

Außerdem können Sie den automatischen Aufgabenstart nach dem Start des Programms aufschieben. Dann werden alle geplanten Aufgaben erst gestartet, nachdem Kaspersky Internet Security gestartet wurde und eine bestimmte Zeit verstrichen ist.

Der spezielle Modus zur Untersuchung im Computerleerlauf (s. Abschnitt "Aufgabenstart im Hintergrundmodus" auf S. 166) erlaubt es, ein automatisches Update dann zu starten, wenn der Computer nicht verwendet wird.

Gehen Sie folgendermaßen vor, um den Startzeitplan für die Updateaufgabe anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Update-Einstellungen**.
3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan**aus und konfigurieren Sie den Startmodus für die Aktualisierung.

Gehen Sie folgendermaßen vor, um den automatischen Start einer übersprungenen Aufgabe zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Update-Einstellungen**.
3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus und aktivieren Sie das Kontrollkästchen **Übersprungene Aufgaben starten**.

Gehen Sie folgendermaßen vor, um den Aufgabenstart nach dem Programmstart aufzuschieben:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Update-Einstellungen**.
3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Zeitplan** die Option **Nach Zeitplan** aus und legen Sie im Feld **Start nach Programmstart aufschieben für** fest, wie lange der Aufgabenstart zurückgestellt werden soll.

ROLLBACK ZUM VORHERIGEN UPDATE

Nach dem ersten Update von Kaspersky Internet Security steht die Funktion für ein Rollback zu der vorherigen Version der Datenbanken zur Verfügung.

Die Rollback-Funktion ist beispielsweise nützlich, wenn die neue Datenbankversion eine fehlerhafte Signatur enthält, die dazu führt, dass Kaspersky Internet Security ein harmloses Programm blockiert.

Wenn die Datenbanken von Kaspersky Internet Security beschädigt sind, wird empfohlen, die Updateaufgabe zu starten, um die aktuellen Datenbanken herunterzuladen.

Gehen Sie folgendermaßen vor, um zur Verwendung der vorhergehenden Version der Datenbanken zurückzukehren:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Update**.
3. Klicken Sie im folgenden Fenster **Update** auf die Schaltfläche ▼ und wählen Sie im folgenden Menü den Punkt **Rollback zu den vorherigen Datenbanken**.

UPDATESTART MIT DEN RECHTEN EINES ANDEREN BENUTZERS

Das Update wird standardmäßig unter dem Benutzerkonto gestartet, mit dessen Rechten Sie sich im System angemeldet haben. Das Update für Kaspersky Internet Security kann aber auch aus einer Quelle erfolgen, auf die Sie keinen Zugriff besitzen (z.B. Netzwerkordner, der Updates enthält) oder für die Sie nicht über Rechte eines autorisierten Benutzers für den Proxyserver verfügen. Sie können das Update von Kaspersky Internet Security unter dem Namen eines Benutzers starten, der über die erforderlichen Privilegien verfügt.

Gehen Sie folgendermaßen vor, um das Update mit den Rechten eines anderen Benutzers zu starten:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Update-Einstellungen**.
3. Klicken Sie auf der rechten Fensterseite auf **Startmodus**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Startmodus** im Block **Benutzer** das Kontrollkästchen **Aufgabe starten mit Rechten des Benutzers**. Geben Sie darunter in den Feldern den Benutzernamen und das Kennwort an.

PROXYSERVER VERWENDEN

Wenn die Internetverbindung über einen Proxyserver erfolgt, müssen seine Einstellungen angepasst werden, um eine korrekte Aktualisierung von Kaspersky Internet Security zu ermöglichen.

Gehen Sie folgendermaßen vor, um die Proxyserver-Einstellungen anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Update-Einstellungen**.
3. Klicken Sie auf der rechten Fensterseite auf **Updatequelle**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Quelle** auf die Schaltfläche **Proxyserver...**.
5. Passen Sie im folgenden Fenster **Proxyserver-Einstellungen** die Einstellungen für den Proxyserver an.

DATEI-ANTI-VIRUS

Datei-Anti-Virus schützt das Dateisystem des Computers vor einer Infektion. Diese Komponente wird beim Hochfahren des Betriebssystems gestartet und befindet sich ständig im Arbeitsspeicher des Computers. Sie untersucht alle Dateien, die auf Ihrem Computer und auf den angeschlossenen Laufwerken geöffnet, gespeichert und gestartet werden, auf Viren und andere bedrohliche Programme.

Sie können einen Schutzbereich erstellen und eine Sicherheitsstufe auswählen (Auswahl von Einstellungen, die die Untersuchungsgenauigkeit beeinflussen).

Wenn ein Benutzer oder ein Programm auf eine Datei des Schutzbereichs zugreift, prüft Datei-Anti-Virus, ob die Datenbanken iChecker und iSwift Informationen über die Datei enthalten, und entscheidet auf Basis dieser Informationen, ob eine Untersuchung der Datei erforderlich ist.

Standardmäßig ist immer die *Signaturanalyse* aktiviert. Dabei werden zur Virensuche die Einträge der Programm-Datenbanken verwendet. Außerdem können heuristische Analyse und unterschiedliche Untersuchungstechnologien eingesetzt werden.

Wenn in einer Datei eine Bedrohung gefunden wird, weist Kaspersky Internet Security der Datei eine der folgenden Statusvarianten zu:

- Status, der den Typ der gefundenen Malware angibt (beispielsweise *Virus* oder *trojanisches Programm*).
- Status *möglicherweise infiziert* (verdächtig), wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob eine Datei infiziert ist oder nicht. Möglicherweise enthält die Datei eine Codefolge, die für Viren oder andere bedrohliche Programme typisch ist, oder die Datei enthält den modifizierten Code eines bekannten Virus.

Anschließend zeigt das Programm eine Meldung (s. S. 182) über die gefundene Bedrohung an und führt mit der Datei die Aktion aus, die in den Einstellungen von Datei-Anti-Virus festgelegt ist. Sie können die Aktion ändern (s. S. 86), die das Programm beim Fund einer Bedrohung ausführen soll.

Wenn Sie im automatischen Modus (s. Abschnitt "Schutzmodus auswählen" auf S. 68) arbeiten, führt Kaspersky Internet Security beim Fund gefährlicher Objekte automatisch die von den Kaspersky-Lab-Experten empfohlenen Aktionen aus. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige – **In die Quarantäne verschieben**. Wenn Sie im interaktiven Modus arbeiten (s. Abschnitt "Schutzmodus auswählen" auf S. 68), zeigt das Programm beim Fund gefährlicher Objekte eine Meldung an, in der Sie die erforderliche Aktion auswählen können.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren. Verdächtige (möglicherweise infizierte) Objekte werden in die Quarantäne verschoben. Sie können eine automatische Untersuchung der Quarantänedateien nach jedem Update festlegen.

IN DIESEM ABSCHNITT

DATEI-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

Datei-Anti-Virus ist standardmäßig aktiviert und arbeitet in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie Datei-Anti-Virus deaktivieren.

Gehen Sie folgendermaßen vor, um Datei-Anti-Virus zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Datei-Anti-Virus aktivieren**.

DATEI-ANTI-VIRUS AUTOMATISCH ANHALTEN

Bei der Ausführung von Arbeiten, die die Betriebssystemressourcen stark beanspruchen, kann die Arbeit von Datei-Anti-Virus vorübergehend angehalten werden. Um die Belastung zu verringern und den schnellen Zugriff auf Objekte zu gewährleisten, kann festgelegt werden, dass die Komponente zu einem bestimmten Zeitpunkt oder bei der Arbeit mit bestimmten Programmen automatisch angehalten wird.

Datei-Anti-Virus bei einem Konflikt mit bestimmten Programmen anzuhalten, gilt als Notlösung! Sollten bei der Ausführung der Komponente Konflikte auftreten, dann wenden Sie sich an den Technischen Support von Kaspersky Lab (http://support.kaspersky.de). Die Spezialisten helfen Ihnen dabei, auf Ihrem Computer die gemeinsame Arbeit von Kaspersky Internet Security mit anderen Programmen einzurichten.

Gehen Sie folgendermaßen vor, damit die Komponente zu einem bestimmten Zeitpunkt angehalten wird:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen **Nach Zeitplan** und klicken Sie auf **Zeitplan**.
5. Geben Sie im Fenster **Aufgabe anhalten** in den Feldern **Anhalten um** und **Fortsetzen um** den erforderlichen Zeitraum an (im Format HH:MM).

Gehen Sie folgendermaßen vor, damit die Komponente beim Start bestimmter Programme angehalten wird:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Aufgabe anhalten** das Kontrollkästchen **Beim Start folgender Programme...** und klicken Sie auf die Schaltfläche **Auswählen...**.
5. Legen Sie im Fenster **Programme** die Liste der Programme an, bei deren Arbeit die Komponente angehalten werden soll.

SCHUTZBEREICH FÜR DATEI-ANTI-VIRUS FESTLEGEN

Ein Schutzbereich legt Ort und Typ der zu untersuchenden Dateien fest. Kaspersky Internet Security untersucht standardmäßig nur potenziell infizierbare Dateien, die von beliebigen Festplatten, Wechseldatenträgern und Netzlaufwerken aus gestartet werden.

➡ *Gehen Sie folgendermaßen vor, um einen Schutzbereich zu erstellen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Geben Sie im folgenden Fenster auf der Registerkarte **Allgemein** unter **Dateitypen** den Typ der Dateien an, die Sie mit Datei-Anti-Virus untersuchen möchten:
   - Wählen Sie **Alle Dateien**, wenn alle Dateien untersucht werden sollen.
   - Wählen Sie **Dateien nach Format untersuchen**, wenn nur Dateien mit den Formate untersucht werden sollen, die am häufigsten infiziert werden.
   - Wählen Sie **Dateien nach Erweiterung untersuchen**, wenn Dateien mit den Erweiterungen untersucht werden sollen, die am häufigsten infiziert werden.

   Bei der Auswahl des Typs für die zu untersuchenden Dateien muss Folgendes beachtet werden:
   - Es gibt eine Reihe von Dateiformaten (z.B. TXT), für die das Risiko des Eindringens von schädlichem Code und dessen späterer Aktivierung relativ gering ist. Gleichzeitig gibt es Formate, die ausführbaren Code enthalten oder enthalten können (EXE, DLL, DOC). Das Risiko, dass schädlicher Code in solche Dateien eindringt und aktiviert wird, ist relativ hoch.
   - Ein Angreifer kann einen Virus oder ein anderes bedrohliches Programm in einer ausführbaren Datei, deren Erweiterung in txt geändert wurde, an Ihren Computer senden. Wenn die Sie die Dateiuntersuchung nach Erweiterung ausgewählt haben, wird eine solche Datei bei der Untersuchung übersprungen. Wurde die Untersuchung von Dateien nach Format gewählt, ignoriert Datei-Anti-Virus die Erweiterung und analysiert die Kopfzeile der Datei, wodurch sich ergeben kann, dass die Datei das Format EXE besitzt. Eine solche Datei wird sorgfältig auf Viren und andere bedrohliche Programme untersucht.
5. Führen Sie in der Liste **Schutzbereich** eine der folgenden Aktionen aus:
   - Wenn Sie der Liste der Untersuchungsobjekte ein neues Objekt hinzufügen möchten, klicken Sie auf den Link **Hinzufügen**.
   - Wenn Sie den Ort für ein Objekt ändern möchten, markieren Sie das Objekt in der Liste und klicken Sie auf den Link **Ändern**.

   Das Fenster **Untersuchungsobjekt wählen** wird geöffnet.
   - Wenn Sie ein Objekt aus der Liste der Untersuchungsobjekte löschen möchten, markieren Sie das Objekt in der Liste und klicken Sie auf den Link **Löschen**.

     Ein Fenster zur Bestätigung des Löschens wird geöffnet.
6. Führen Sie eine der folgenden Aktionen aus:
   - Wenn Sie der Liste der Untersuchungsobjekte ein neues Objekt hinzufügen möchten, markieren Sie das Objekt im Fenster **Untersuchungsobjekt wählen** und klicken Sie auf **OK**.
   - Wenn Sie den Ort für ein Objekt ändern möchten, ändern Sie im Fenster **Untersuchungsobjekt wählen** unter **Objekt** den Pfad des Objekts und klicken Sie auf **OK**.
   - Wenn Sie ein Objekt aus der Liste der Untersuchungsobjekte löschen möchten, klicken Sie im Bestätigungsfenster auf **Ja**.
7. Wiederholen Sie gegebenenfalls die Punkte 6-7, um ein Objekt hinzuzufügen, den Ort eines Objekts zu ändern oder Objekte aus der Liste der Untersuchungsobjekte zu löschen.

8. Wenn ein Objekt aus der Liste der Untersuchungsobjekte ausgeschlossen werden soll, deaktivieren Sie in der Liste **Schutzbereich** das entsprechende Kontrollkästchen. In diesem Fall verbleibt das Objekt in der Liste der Untersuchungsobjekte, wird aber von Datei-Anti-Virus aus der Untersuchung ausgeschlossen.

SICHERHEITSSTUFE FÜR DATEIEN ÄNDERN UND WIEDERHERSTELLEN

Abhängig von den aktuellen Erfordernissen können Sie eine vordefinierte Stufe für die Sicherheit von Dateien und Speicher wählen oder die Einstellungen von Datei-Anti-Virus entsprechend anpassen.

Während der Konfiguration von Datei-Anti-Virus können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese Einstellungen gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und entsprechen der Sicherheitsstufe **Empfohlen**.

➧ *Gehen Sie folgendermaßen vor, um die Sicherheitsstufe für Dateien zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Stellen Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

   Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

➧ *Gehen Sie folgendermaßen vor, um die standardmäßige Sicherheitssstufe für Dateien wiederherzustellen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

UNTERSUCHUNGSMODUS FÜR DATEIEN WÄHLEN

Ein *Untersuchungsmodus* ist eine Bedingung, unter der Datei-Anti-Virus mit der Untersuchung von Dateien beginnt. Kaspersky Internet Security verwendet standardmäßig den intelligenten Modus. Um zu entscheiden, ob eine Untersuchung von Dateien erforderlich ist, berücksichtigt Datei-Anti-Virus in diesem Untersuchungsmodus den Dateiyp und analysiert die Operationen, die ein Benutzer mit einem Objekt ausführt. Beispielsweise untersucht Kaspersky Internet Security bei der Arbeit mit einem Microsoft Office-Dokument eine Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

➧ *Gehen Sie folgendermaßen vor, um den Untersuchungsmodus für Dateien zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungsmodus** den erforderlichen Modus.

   Bei der Auswahl eines Untersuchungsmodus muss berücksichtigt werden, mit welcher Art von Dateien Sie überwiegend arbeiten.

HEURISTISCHE ANALYSE FÜR DATEI-ANTI-VIRUS VERWENDEN

Bei der Arbeit von Datei-Anti-Virus wird immer die Methode *Signaturanalyse* verwendet, bei der Kaspersky Internet Security ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht.

Um die Effektivität des Schutzes zu steigern, können Sie eine *heuristische Analyse* verwenden (Analyse der Aktivität, die ein Objekt im System zeigt). Diese Analyse erlaubt die Erkennung neuer Schadobjekte, über die noch keine Datenbankeinträge vorliegen.

➧ *Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Leistung** im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter die Genauigkeitsstufe der Untersuchung ein.

TECHNOLOGIEN FÜR DIE DATEIUNTERSUCHUNG AUSWÄHLEN

Zusätzlich zur heuristischen Analyse können Sie spezielle Technologien einsetzen, mit denen sich die Dateiuntersuchung beschleunigen lässt. Dabei werden Dateien von der Untersuchung ausgeschlossen, die seit dem letzten Scan nicht verändert wurden.

➧ *Gehen Sie folgendermaßen vor, um die Technologien zur Objektuntersuchung zu wählen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Untersuchungstechnologien** die gewünschten Werte.

AKTION FÜR INFIZIERTE DATEIEN ÄNDERN

Beim Fund von infizierten Objekten führt das Programm eine festgelegte Aktion aus.

➧ *Gehen Sie folgendermaßen vor, um die Aktion für infizierte Dateien zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Wählen Sie auf der rechten Fensterseite im Block **Aktion beim Fund einer Bedrohung** die entsprechende Option aus.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN DURCH DATEI-ANTI-VIRUS

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie beispielsweise Archive, Installationspakete, angehängte OLE-Objekte und Dateien in Mailformaten. Um Viren zu

erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Für jeden Typ einer zusammengesetzten Datei können Sie wählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie zur Auswahl den Link neben dem Namen des Objekts. Er verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn der Modus gewählt wurde, in dem nur neue und veränderte Dateien untersucht werden, stehen die Links zur Auswahl aller oder nur neuer Dateien nicht zur Verfügung.

In der Grundeinstellung untersucht Kaspersky Internet Security nur angehängte OLE-Objekte.

Bei der Untersuchung von umfangreichen zusammengesetzten Dateien kann das vorausgehende Entpacken viel Zeit beanspruchen. Diese Dauer kann reduziert werden, wenn die Untersuchung von Dateien, die eine bestimmte Größe überschreiten, im Hintergrundmodus erfolgt. Wenn bei der Arbeit mit einer solchen Datei ein schädliches Objekt gefunden wird, werden Sie von Kaspersky Internet Security darüber informiert.

Außerdem können Sie festlegen, bis zu welcher maximalen Größe eine zusammengesetzte Datei untersucht werden soll. Zusammengesetzte Dateien, die den festgelegten Wert überschreiten, werden nicht untersucht.

Wenn umfangreiche Dateien aus Archiven extrahiert werden, erfolgt eine Untersuchung auch dann, wenn das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** aktiviert ist.

Gehen Sie folgendermaßen vor, um die Liste der zu untersuchenden zusammengesetzten Dateien zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** die Typen der zusammengesetzten Dateien, die untersucht werden sollen.

Gehen Sie folgendermaßen vor, um eine maximale Größe für zusammengesetzte Dateien festzulegen, die untersucht werden sollen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.
5. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Große zusammengesetzte Dateien nicht entpacken** und legen Sie eine maximale Größe für zu untersuchende Dateien fest.

Gehen Sie folgendermaßen vor, damit umfangreiche zusammengesetzte Dateien im Hintergrundmodus entpackt werden:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung von zusammengesetzten Dateien** auf die Schaltfläche **Erweitert**.
5. Aktivieren Sie im Fenster **Zusammengesetzte Dateien** das Kontrollkästchen **Zusammengesetzte Dateien im Hintergrund entpacken** und legen Sie eine minimale Dateigröße fest.

DATEIUNTERSUCHUNG OPTIMIEREN

Sie können die Untersuchungsdauer verkürzen und die Arbeitsgeschwindigkeit von Kaspersky Internet Security erhöhen. Dies lässt sich erreichen, wenn nur neue Dateien und Dateien, die seit der letzten Analyse verändert wurden, untersucht werden. Dieser Untersuchungsmodus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

➨ *Gehen Sie folgendermaßen vor, damit nur neue und veränderte Dateien untersucht werden:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Datei-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Leistung** im Block **Untersuchung optimieren** das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**.

MAIL-ANTI-VIRUS

Mail-Anti-Virus untersucht, ob in ein- und ausgehenden E-Mails gefährliche Objekte vorhanden sind. Diese Komponente wird beim Start des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle E-Mail-Nachrichten, die über die Protokolle POP3, SMTP, IMAP, MAPI und NNTP sowie über geschützte Verbindungen (SSL) über die Protokolle POP3 und IMAP übertragen werden (s. Abschnitt "Untersuchung geschützter Verbindungen" auf S. 123).

Als Indikator für die Arbeit der Komponente dient das Symbol im Infobereich der Taskleiste, das jedes Mal bei der Untersuchung einer E-Mail das Aussehen annimmt.

Jede E-Mail-Nachricht, die von einem Benutzer empfangen oder gesendet wird, wird von Mail-Anti-Virus abgefangen und untersucht. Wenn in einer E-Mail keine Bedrohungen gefunden werden, erhält der Benutzer Zugriff auf die Nachricht.

Sie können die Nachrichtentypen angeben, die untersucht werden sollen, und eine Sicherheitsstufe90 (s. S.) wählen (Auswahl von Einstellungen für die Untersuchungsgenauigkeit).

Standardmäßig ist immer die *Signaturanalyse* aktiviert. Dabei werden zur Virensuche die Einträge der Programm-Datenbanken verwendet. Zusätzlich kann die heuristische Analyse eingesetzt werden. Außerdem können Sie die Anlagenfilterung (s. S. 91) aktivieren, mit der Dateien bestimmter Typen automatisch umbenannt oder gelöscht werden können.

Wenn in einer Datei eine Bedrohung gefunden wird, weist Kaspersky Internet Security der Datei eine der folgenden Statusvarianten zu:

- Status, der den Typ der gefundenen Malware angibt (beispielsweise *Virus* oder *trojanisches Programm*).
- Status *möglicherweise infiziert* (verdächtig), wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob eine Datei infiziert ist oder nicht. Möglicherweise enthält die Datei eine Codefolge, die für Viren oder andere bedrohliche Programme typisch ist, oder die Datei enthält den modifizierten Code eines bekannten Virus.

Anschließend blockiert das Programm die E-Mail-Nachricht, zeigt eine Meldung (s. S. 182) über den Fund der Bedrohung an und führt die in den Einstellungen von Mail-Anti-Virus festgelegte Aktion aus. Sie können die Aktion beim Fund einer Bedrohung ändern (s. Abschnitt "Aktion für infizierte E-Mail-Nachrichten ändern" auf S. 91).

Wenn Sie im automatischen Modus (s. Abschnitt "Schutzmodus auswählen" auf S. 68) arbeiten, führt Kaspersky Internet Security beim Fund gefährlicher Objekte automatisch die von den Kaspersky-Lab-Experten empfohlenen Aktionen aus. Für schädliche Objekte ist dies die Aktion **Desinfizieren. Löschen, wenn Desinfektion nicht möglich**, für verdächtige – **In die Quarantäne verschieben**. Wenn Sie im interaktiven Modus arbeiten (s. Abschnitt "Schutzmodus auswählen" auf S. 68), zeigt das Programm beim Fund gefährlicher Objekte eine Meldung an, in der Sie die erforderliche Aktion auswählen können.

Bevor ein infiziertes Objekt desinfiziert oder gelöscht wird, legt Kaspersky Internet Security eine Sicherungskopie des Objekts an. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren. Verdächtige (möglicherweise infizierte) Objekte werden in die Quarantäne verschoben. Sie konnen festlegen, dass die Quarantanedateien nach jedem Update automatisch untersucht werden.

Wenn die Desinfektion erfolgreich verläuft, wird der Zugriff auf die E-Mail-Nachricht freigegeben. Wenn die Desinfektion fehlschlägt, wird das infizierte Objekt aus der E-Mail-Nachricht gelöscht. Mail-Anti-Virus fügt dem Betreff der E-Mail einen Text hinzu, der darüber informiert, dass die E-Mail von Kaspersky Internet Security verarbeitet wurde.

Für das Mailprogramm Microsoft Office Outlook ist ein integrierbares Erweiterungsmodul vorgesehen, das die Feineinstellung der E-Mail-Untersuchung erlaubt.

Wenn Sie das Mailprogramm The Bat! verwenden, kann Kaspersky Internet Security zusammen mit anderen Antiviren-Anwendungen benutzt werden. Dabei werden die Regeln zur Verarbeitung des Mailverkehrs direkt im Programm The Bat! erstellt und besitzen Vorrang gegenüber den E-Mail-Schutz-Einstellungen von Kaspersky Internet Security.

Bei der Arbeit mit anderen gängigen Mailprogrammen (einschließlich Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail) untersucht Mail-Anti-Virus den Mailverkehr der Protokolle SMTP, POP3, IMAP und NNTP bei Empfang bzw. Versand.

Beachten Sie, dass bei der Arbeit mit dem Mailprogramm Thunderbird E-Mails, die mit dem IMAP- Protokoll übertragen werden, nicht auf Viren untersucht werden, wenn Filter verwendet werden, die Nachrichten aus dem Ordner **Posteingang** verschieben.

IN DIESEM ABSCHNITT

MAIL-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

Mail-Anti-Virus ist standardmäßig aktiviert und arbeitet in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie Mail-Anti-Virus deaktivieren.

Gehen Sie folgendermaßen vor, um Mail-Anti-Virus zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Mail-Anti-Virus aktivieren**.

SCHUTZBEREICH FÜR MAIL-ANTI-VIRUS FESTLEGEN

Ein Schutzbereich umfasst folgende Aspekte: Typ der zu untersuchenden E-Mails; Protokolle, deren Datenverkehr von Kaspersky Internet Security untersucht wird; sowie Einstellungen für die Integration von Mail-Anti-Virus in das System.

Kaspersky Internet Security untersucht standardmäßig ein- und ausgehende E-Mails, integriert ein Plug-in in die Mailprogramme Microsoft Office Outlook und The Bat!, und untersucht den Datenverkehr der Mailprotokolle POP3, SMTP, NNTP und IMAP.

➡ *Gehen Sie folgendermaßen vor, um die Untersuchung ausgehender E-Mails auszuschalten:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Allgemein** im Block **Schutzbereich** die Variante **Nur eingehende Nachrichten**.

Wenn Sie nur die Untersuchung eingehender E-Mails ausgewählt haben, sollte gleich zu Beginn der Arbeit mit Kaspersky Internet Security die ausgehende Mail untersucht werden, da sich auf Ihrem Computer Mailwürmer befinden können, die E-Mails als Ausbreitungskanal verwenden. Eine Untersuchung der ausgehenden Mail verhindert Probleme, die auftreten können, wenn von Ihrem Computer aus unkontrolliert infizierte E-Mails verschickt werden.

➡ *Gehen Sie folgendermaßen vor, um die zu untersuchenden Protokolle und die Einstellungen für die Integration von Mail-Anti-Virus in das System festzulegen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Integration ins System** die erforderlichen Einstellungen.

SICHERHEITSSTUFE FÜR E-MAILS ÄNDERN UND WIEDERHERSTELLEN

Abhängig von den aktuellen Erfordernissen können Sie eine vordefinierte Sicherheitsstufe für E-Mails wählen oder die Einstellungen von Mail-Anti-Virus entsprechend anpassen.

Die Spezialisten von Kaspersky Lab warnen davor, die Einstellungen von Mail-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, eine andere Sicherheitsstufe zuwählen.

Während der Konfiguration von Mail-Anti-Virus können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese Einstellungen gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und entsprechen der Sicherheitsstufe **Empfohlen**.

➡ *Gehen Sie folgendermaßen vor, um die festgelegte Sicherheitsstufe für E-Mails zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.

3. Stellen Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

   Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für den Mail-Schutz wiederherzustellen,

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

HEURISTISCHE ANALYSE FÜR MAIL-ANTI-VIRUS VERWENDEN

Bei der Arbeit von Mail-Anti-Virus wird immer die Methode *Signaturanalyse* verwendet, bei der Kaspersky Internet Security ein gefundenes Objekt mit den Einträgen in den Datenbanken vergleicht.

Um die Effektivität des Schutzes zu steigern, können Sie eine *heuristische Analyse* verwenden (Analyse der Aktivität, die ein Objekt im System zeigt). Diese Analyse erlaubt die Erkennung neuer Schadobjekte, über die noch keine Datenbankeinträge vorliegen.

Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Allgemein** im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter die Genauigkeitsstufe der Untersuchung ein.

AKTION FÜR INFIZIERTE E-MAIL-NACHRICHTEN ÄNDERN

Beim Fund von infizierten Objekten führt das Programm eine festgelegte Aktion aus.

Gehen Sie folgendermaßen vor, um die Aktion für infizierte E-Mails zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Wählen Sie auf der rechten Fensterseite im Block **Aktion beim Fund einer Bedrohung** die entsprechende Option aus.

ANLAGENFILTERUNG IN E-MAIL-NACHRICHTEN

Schädliche Programme können per E-Mail als Nachrichtenanhänge verbreitet werden. Sie können eine Filterung nach dem Typ der E-Mail-Anlagen anpassen. Dadurch werden Dateien der festgelegten Typen automatisch umbenannt oder gelöscht.

Gehen Sie folgendermaßen vor, um die Anlagenfilterung anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Anlagenfilterung** einen Filtermodus. Bei Auswahl der letzten beiden Modi wird die Liste der Dateitypen (Erweiterungen) aktiviert. In dieser Liste können Sie die erforderlichen Typen wählen oder die Maske eines neuen Typs hinzufügen.

   Um der Liste einen neuen Maskentyp hinzuzufügen, klicken Sie auf den Link **Hinzufügen**, öffnen Sie das Fenster **Maske für einen Dateinamen** und geben Sie dort die erforderlichen Daten ein.

UNTERSUCHUNG VON ZUSAMMENGESETZTEN DATEIEN DURCH MAIL-ANTI-VIRUS

Eine häufige Methode zum Verstecken von Viren ist das Eindringen von Schädlingen in zusammengesetzte Dateien wie beispielsweise Archive, Installationspakete, angehängte OLE-Objekte und Dateien in Mailformaten. Um Viren zu erkennen, die auf diese Weise versteckt wurden, muss eine zusammengesetzte Datei entpackt werden. Dadurch kann das Untersuchungstempo wesentlich sinken.

Sie können die Untersuchung von zusammengesetzten Dateien aktivieren oder deaktivieren, sowie die maximale Größe der zu untersuchenden zusammengesetzten Dateien begrenzen.

Wenn Ihr Computer nicht durch die Mittel eines lokalen Netzwerks geschützt ist (d.h. die Internetverbindung ohne Proxyserver oder Firewall erfolgt), wird davor gewarnt, die Untersuchung von zusammengesetzten Dateien zu deaktivieren.

Gehen Sie folgendermaßen vor, um die Untersuchung von zusammengesetzten Dateien anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Mail-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Geben Sie im folgenden Fenster auf der Registerkarte **Allgemein** die entsprechenden Parameter an.

E-MAIL-UNTERSUCHUNG IN MICROSOFT OFFICE OUTLOOK

Bei der Installation von Kaspersky Internet Security wird ein spezielles Plug-in in das Programm Microsoft Office Outlook integriert. Es erlaubt, aus dem Mailprogramm Microsoft Office Outlook schnell zu den Einstellungen für Mail-Anti-Virus zu gelangen, und festzulegen, wann Mail-Anti-Virus E-Mails auf Viren und andere bedrohliche Programme untersuchen soll (beim Empfang, Öffnen oder Senden).

Mail-Anti-Virus kann vom Programm Microsoft Office Outlook aus angepasst werden, wenn diese Option in den Einstellungen für den Schutzbereich von Mail-Anti-Virus ausgewählt wurde.

Gehen Sie folgendermaßen vor, um im Programm Microsoft Office Outlook die E-Mail-Untersuchung anzupassen:

1. Öffnen Sie das Hauptfenster von Microsoft Office Outlook.
2. Wählen Sie im Programmmenü den Punkt **Extras** → **Optionen**.
3. Wählen Sie im folgenden Fenster **Einstellungen** die Registerkarte **E-Mail-Schutz**.

E-MAIL-UNTERSUCHUNG IN THE BAT!

Die Aktionen für infizierte E-Mail-Objekte werden im Mailprogramm The Bat! durch Mittel des Programms festgelegt.

Die Einstellungen von Mail-Anti-Virus, die festlegen, ob ein- und ausgehende E-Mails untersucht werden oder nicht, und die Aktionen für gefährliche E-Mail-Objekte und Ausnahmen bestimmen, werden ignoriert. Das Programm The Bat! berücksichtigt lediglich die Untersuchung angehängter Archive.

Die Parameter für den E-Mail-Schutz gelten für alle auf dem Computer installierten Antiviren-Komponenten, die die Arbeit mit The Bat! unterstützen.

Es sollte beachtet werden, dass E-Mails beim Empfang zuerst von Mail-Anti-Virus untersucht werden und erst anschließend von dem Plug-in des Mailprogramms The Bat!. Wenn ein schädliches Objekt gefunden wird, werden Sie von Kaspersky Internet Security auf jeden Fall darüber informiert. Wenn dabei im Meldungsfenster von Mail-Anti-Virus die Aktion Desinfizieren (Löschen) gewählt wird, führt Mail-Anti-Virus das Löschen der Bedrohung aus. Wird im Meldungsfenster die Aktion Überspringen gewählt, so wird das Objekt von dem Plug-in für The Bat! desinfiziert. Beim Senden werden E-Mails zuerst von dem Plug-in und anschließend von Mail-Anti-Virus untersucht.

Mail-Anti-Virus kann vom Programm The Bat! aus angepasst werden, wenn diese Option in den Einstellungen für den Schutzbereich von Mail-Anti-Virus ausgewählt wurde.

Legen Sie folgende Kriterien fest, um die E-Mail-Untersuchung in The Bat! anzupassen:

- Welche Richtung des E-Mail-Verkehrs (eingehend, ausgehend) der Virenuntersuchung unterzogen werden soll.
- Wann die Untersuchung von Mail-Objekten erfolgen soll (beim Öffnen einer Mail oder vor dem Speichern auf der Festplatte).
- Welche Aktionen das Mailprogramm ausführen soll, wenn gefährliche Objekte gefunden werden. Es stehen beispielsweise zur Auswahl:
  - **Reparaturversuch infizierter Teile** – Bei Auswahl dieser Variante wird versucht, ein infiziertes Objekt zu desinfizieren. Wenn die Desinfektion fehlschlägt, verbleibt das Objekt in der Nachricht.
  - **Infizierte Teile löschen** – Bei Auswahl dieser Variante wird ein gefährliches E-Mail-Objekt gelöscht. Dabei bleibt unberücksichtigt, ob es infiziert ist oder als verdächtig gilt.

Standardmäßig verschiebt das Programm The Bat! alle infizierten E-Mail-Objekte ohne Desinfektion in die Quarantäne.

E-Mail-Nachrichten, die gefährliche Objekte enthalten, werden bei einer Untersuchung im Mailprogramm The Bat! nicht durch eine spezielle Kopfzeile gekennzeichnet.

Gehen Sie folgendermaßen vor, um im Programm The Bat! die E-Mail-Untersuchung anzupassen:

1. Öffnen Sie das Hauptfenster des Programms The Bat!.
2. Wählen Sie im Menü **Eigenschaften** den Punkt **Einstellungen**.
3. Wählen Sie in der Konfigurationsstruktur das Objekt **Virenschutz**.

WEB-ANTI-VIRUS

Bei der Arbeit im Internet besteht für die Informationen, die auf Ihrem Computer gespeichert sind, das Risiko einer Infektion durch Viren und andere bedrohliche Programme. Diese können in Ihren Computer eindringen, wenn Sie kostenlose Programme herunterladen oder Webseiten besuchen, die zuvor von Hackern angegriffen worden sind.

Außerdem können Netzwürmer direkt beim Aufbau einer Internetverbindung in Ihren Computer eindringen, noch bevor eine Webseite geöffnet oder eine Datei heruntergeladen wurde.

Web-Anti-Virus schützt Informationen, die über das HTTP-, HTTPS- und FTP-Protokoll auf Ihren Computer gelangen oder von ihm gesendet werden. Außerdem verhindert er, dass auf Ihrem Computer gefährliche Skripte gestartet werden.

Web-Anti-Virus kontrolliert nur den Web-Datenverkehr, der über die Ports abgewickelt wird, die auf der Liste der zu kontrollierenden Ports stehen. Eine Liste der zu kontrollierenden Ports, die am häufigsten zur Datenübertragung dienen, gehört zum Lieferumfang von Kaspersky Internet Security. Wenn Sie Ports verwenden, die nicht auf der Liste der zu kontrollierenden Ports stehen, fügen Sie diese zur Liste der zu kontrollierenden Ports hinzu (s. Abschnitt "Liste der zu kontrollierenden Ports erstellen" auf S. 126), um den Schutz des darüber abgewickelten Web-Datenverkehrs sicherzustellen.

Web-Anti-Virus untersucht den Web-Datenverkehr mit einer bestimmten Auswahl von Einstellungen, die als Sicherheitsstufe bezeichnet wird. Beim Fund von Bedrohungen führt Web-Anti-Virus die festgelegte Aktion aus. Die Suche nach schädlichen Objekten erfolgt auf Basis der Datenbanken, die bei der Arbeit von Kaspersky Internet Security verwendet werden, sowie mit Hilfe eines heuristischen Algorithmus.

Die Spezialisten von Kaspersky Lab warnen davor, die Funktionsparameter von Web-Anti-Virus zu verändern. In den meisten Fällen ist es ausreichend, eine passende Sicherheitsstufe zu wählen.

Algorithmus für die Untersuchung des Web-Datenverkehrs

Jede Webseite oder Datei, auf die Sie oder ein bestimmtes Programm über die Protokolle HTTP, HTTPS oder FTP zugreifen, wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert.

- Wenn eine Webseite oder eine Datei, auf die ein Benutzer zugreift, schädlichen Code enthält, wird der Zugriff darauf blockiert. Dabei erscheint auf dem Bildschirm eine Meldung darüber, dass die angeforderte Datei oder die Seite infiziert ist.
- Wenn die Datei oder Webseite keinen schädlichen Code enthält, erhält der Benutzer sofort Zugriff darauf.

Algorithmus für die Skript-Untersuchung

Jedes auszuführende Skript wird von Web-Anti-Virus abgefangen und auf schädlichen Code analysiert.

- Wenn ein Skript schädlichen Code enthält, blockiert Web-Anti-Virus das Skript und zeigt eine Meldung an.
- Wenn im Skript kein schädlicher Code gefunden wird, wird es ausgeführt.

Web-Anti-Virus fängt nur Skripte ab, die auf der Technologie Microsoft Windows Script Host basieren.

IN DIESEM ABSCHNITT

WEB-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

Web-Anti-Virus ist standardmäßig aktiviert und arbeitet in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie Web-Anti-Virus deaktivieren.

Gehen Sie folgendermaßen vor, um Web-Anti-Virus zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Web-Anti-Virus aktivieren**.

SICHERHEITSSTUFE FÜR DEN WEB-DATENVERKEHR ÄNDERN UND WIEDERHERSTELLEN

Abhängig von den aktuellen Erfordernissen können Sie eine vordefinierte Sicherheitsstufe für den Web-Datenverkehr auswählen oder die Einstellungen von Web-Anti-Virus entsprechend anpassen.

Während der Konfiguration von Web-Anti-Virus können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese Einstellungen gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und entsprechen der Sicherheitsstufe **Empfohlen**.

Gehen Sie folgendermaßen vor, um die Sicherheitsstufe für den Web-Datenverkehr zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Stellen Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

   Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die standardmäßige Sicherheitssstufe für den Web-Datenverkehr wiederherzustellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

AKTION FÜR GEFÄHRLICHE OBJEKTE IM WEB-DATENVERKEHR ÄNDERN

Beim Fund von infizierten Objekten führt das Programm eine festgelegte Aktion aus.

Was die Aktionen für gefährliche Skripte betrifft, so sperrt Web-Anti-Virus deren Ausführung immer und zeigt auf dem Bildschirm eine Meldung an, die den Benutzer über die ausgeführte Aktion informiert. Die Aktion für ein gefährliches Skript kann nicht geändert werden, es ist nur möglich, die Skript-Untersuchung zu deaktivieren (s. Abschnitt "Gefährliche Skripte blockieren" auf S. 99).

➡ *Gehen Sie folgendermaßen vor, um die Aktion für gefundene Objekte zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Wählen Sie auf der rechten Fensterseite im Block **Aktion beim Fund einer Bedrohung** die entsprechende Option aus.

LINKS AUF WEBSEITEN PRÜFEN

Eine Phishing-Prüfung von Links auf Webseiten erlaubt es, *Phishing-Angriffe* zu vermeiden. Phishing-Angriffe besitzen in der Regel die Form von E-Mails, die scheinbar von Kreditinstituten stammen und Links auf deren Webseiten enthalten. Eine solche Nachricht fordert dazu auf, einem Link zu folgen und auf der betreffenden Webseite vertrauliche Informationen einzugeben, wie beispielsweise eine Kreditkartennummer oder Benutzername und Kennwort für ein Online-Banking-Konto. Ein häufiges Beispiel für Phishing-Angriffe ist eine Nachricht, die scheinbar von einer Bank stammt, bei der Sie Kunde sind, und einen Link zu der offiziellen Webseite der Bank enthält. Wenn Sie dem Link folgen, gelangen Sie auf eine Webseite, die eine genaue Kopie der Bankseite darstellt und im Browser sogar deren Adresse anzeigen kann, obwohl Sie sich in Wirklichkeit auf einer fiktiven Webseite befinden. Alle Aktionen, die Sie auf dieser Webseite ausführen, werden verfolgt und können zum Diebstahl Ihres Geldes missbraucht werden.

Da sich ein Phishing-Link nicht nur in E-Mails, sondern beispielsweise auch im Text einer ICQ-Nachricht befinden kann, überwacht Web-Anti-Virus alle Versuche zum Öffnen einer Phishing-Seite auf der Ebene des Web-Datenverkehrs und blockiert den Zugriff auf solche Webseiten.

Neben den Kaspersky Internet Security Datenbanken lässt sich zur Untersuchung von Webseiten die Heuristische Analyse (s. S. 98) verwenden.

IN DIESEM ABSCHNITT

LINK-UNTERSUCHUNG AKTIVIEREN UND DEAKTIVIEREN

➡ *Gehen Sie folgendermaßen vor, um die Link-Untersuchung unter Verwendung der Datenbanken für verdächtige Webadressen und Phishing-Webadressen zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Allgemein** im Block **Links untersuchen** die Kontrollkästchen **Links mit Datenbank für verdächtige Webadressen untersuchen** und **Webseiten auf Phishing prüfen**.

MODUL ZUR LINK-UNTERSUCHUNG VERWENDEN

Das Modul zur Link-Untersuchung wird als Plug-in in die Webbrowser Microsoft Internet Explorer, Mozilla Firefox und Google Chrome integriert.

Das Modul untersucht alle Links auf einer geöffneten Webseite. Es wird geprüft, ob Links zu verdächtigen Webadressen gehören oder zum Phishing dienen. Erkannte Links werden im Browserfenster farblich hervorgehoben.

Für die Link-Untersuchung stehen folgende Optionen zur Auswahl: Es kann eine Liste mit Webseiten angelegt werden, auf denen Links untersucht werden sollen; Links werden auf allen Webseiten untersucht, wobei eine Ausnahmeliste möglich ist; Es werden nur Links in Suchergebnissen untersucht; Es werden Webseiten-Kategorien festgelegt, für die Links untersucht werden sollen.

Das Modul zur Link-Untersuchung kann nicht nur im Programmkonfigurationsfenster, sondern auch im Konfigurationsfenster des Moduls angepasst werden. Letzteres wird vom Webbrowser aus geöffnet.

➡ *Gehen Sie folgendermaßen vor, um Webseiten anzugeben, auf denen Links untersucht werden sollen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Das Fenster **Web-Anti-Virus** wird geöffnet.
5. Aktivieren Sie auf der Registerkarte **Web-Filter** im Block **Modul zur Link-Untersuchung** das Kontrollkästchen **Link-Untersuchung aktivieren**.
6. Wählen Sie die Webseiten aus, auf denen Links untersucht werden sollen:
   a. Wählen Sie die Variante **Nur Webseiten aus der Liste** und klicken Sie auf **Festlegen...**, wenn Sie eine Liste mit Webseiten anlegen möchten, auf denen Links untersucht werden sollen. Erstellen Sie im folgenden Fenster **Zu untersuchende Webadressen** eine Liste mit zu prüfenden Webseiten.
   b. Wählen Sie die Variante **Alle, außer Ausnahmen** und klicken Sie auf **Ausnahmen...**, wenn Links auf allen Webseiten untersucht werden sollen, außer den in einer Ausnahmeliste genannten Seiten. Legen Sie im folgenden Fenster **Ausnahmen** eine Liste mit Webseiten an, auf denen Links nicht untersucht werden sollen.

➡ *Gehen Sie folgendermaßen vor, damit nur Links in Suchergebnissen geprüft werden:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Das Fenster **Web-Anti-Virus** wird geöffnet.
5. Aktivieren Sie auf der Registerkarte **Web-Filter** im Block **Modul zur Link-Untersuchung** das Kontrollkästchen **Link-Untersuchung aktivieren** und klicken Sie auf **Einstellungen**.
6. Wählen Sie im folgenden Fenster **Modul zur Link-Untersuchung anpassen** im Block **Untersuchungsmodus** die Variante **Nur Links in Suchergebnissen**.

➡ *Gehen Sie folgendermaßen vor, um die Webseiten-Kategorien auszuwählen, für die Links untersucht werden sollen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Das Fenster **Web-Anti-Virus** wird geöffnet.

5. Aktivieren Sie auf der Registerkarte **Web-Filter** im Block **Modul zur Link-Untersuchung** das Kontrollkästchen **Link-Untersuchung aktivieren** und klicken Sie auf **Einstellungen**.

6. Aktivieren Sie im folgenden Fenster **Modul zur Link-Untersuchung anpassen** im Block **Webseiten-Kategorien** das Kontrollkästchen **Informationen über Kategorien für Webseiten-Inhalte anzeigen**.

7. Aktivieren Sie in der Kategorienliste die Kontrollkästchen für die Webseiten-Kategorien, für die Links untersucht werden sollen.

➧ *Um das Konfigurationsfenster für die Link-Untersuchung aus dem Webbrowser zu öffnen,*

klicken Sie in der Symbolleiste des Browsers auf die Schaltfläche mit dem Symbol von Kaspersky Internet Security.

ZUGRIFF AUF GEFÄHRLICHE WEBSEITEN BLOCKIEREN

Sie können den Zugriff auf Webseiten blockieren, die vom Modul zur Link-Untersuchung als verdächtig oder als Phishing-Seiten eingestuft wurden (s. Abschnitt "Modul zur Link-Untersuchung verwenden" auf S. 97).

➧ *Gehen Sie folgendermaßen vor, um den Zugriff auf gefährliche Webseiten zu blockieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Web-Filter** im Block **Gefährliche Webseiten blockieren** das Kontrollkästchen **Gefährliche Webseiten blockieren**.

HEURISTISCHE ANALYSE FÜR WEB-ANTI-VIRUS VERWENDEN

Um die Effektivität des Schutzes zu steigern, können Sie eine *heuristische Analyse* verwenden (Analyse der Aktivität, die ein Objekt im System zeigt). Diese Analyse erlaubt die Erkennung neuer Schadobjekte, über die noch keine Datenbankeinträge vorliegen.

Die heuristische Analyse lässt sich in Web-Anti-Virus separat für die Untersuchung des Web-Datenverkehrs und für die Phishing-Prüfung von Webseiten aktivieren.

➧ *Gehen Sie folgendermaßen vor, um die heuristische Analyse für die Untersuchung des Web-Datenverkehrs zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** im Block **Heuristische Analyse** das Kontrollkästchen **Heuristische Analyse verwenden** und legen Sie eine Genauigkeitsstufe für die Untersuchung fest.

➡ *Gehen Sie folgendermaßen vor, um die heuristische Analyse für die Phishing-Prüfung von Webseiten zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.
4. Klicken Sie auf der Registerkarte **Allgemein** im Block **Links untersuchen** auf **Erweitert**.
5. Aktivieren Sie im folgenden Fenster **Anti-Phishing anpassen** das Kontrollkästchen **Heuristische Analyse zur Phishing-Prüfung von Webseiten verwenden** und legen Sie eine Genauigkeitsstufe für die Untersuchung fest.

GEFÄHRLICHE SKRIPTE BLOCKIEREN

Web-Anti-Virus untersucht alle Skripte, die in Microsoft Internet Explorer verarbeitet werden, und alle WSH-Skripte (z.B. JavaScript, Visual Basic Script usw.), die ein Benutzer auf dem Computer startet. Wenn ein Skript den Computer gefährden kann, wird seine Ausführung blockiert.

➡ *Gehen Sie folgendermaßen vor, um die Blockierung gefährlicher Skripte zu deaktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.
4. Deaktivieren Sie auf der Registerkarte **Allgemein** im Block **Erweitert** das Kontrollkästchen **Gefährliche Skripte in Microsoft Internet Explorer blockieren**.

UNTERSUCHUNG OPTIMIEREN

Um die Erkennungseffektivität für schädlichen Code zu steigern, wendet Web-Anti-Virus eine Zwischenspeicherung von Objektfragmenten an, die aus dem Internet eintreffen. Wenn die Zwischenspeicherung verwendet wird, untersucht Web-Anti-Virus Objekte erst, nachdem sie vollständig auf den Computer heruntergeladen wurden.

Die Zwischenspeicherung erhöht die Verarbeitungs- und Bereitstellungsdauer für Objekte. Außerdem kann es durch die Zwischenspeicherung zu Problemen beim Laden und bei der Verarbeitung großer Objekte kommen, die mit einer Zeitüberschreitung für die Verbindung zum HTTP-Client zusammenhängen.

Um dieses Problem zu lösen, kann die Zwischenspeicherungsdauer für aus dem Internet heruntergeladene Dateifragmente begrenzt werden. Bei Überschreitung der festgelegten Dauer wird jeder heruntergeladene Teil eines Objekts ungeprüft bereitgestellt. Nach Abschluss des Downloads wird das Objekt vollständig gescannt. Dadurch lässt sich die Bereitstellungsdauer für Objekte reduzieren und das Problem einer Verbindungstrennung lösen. Gleichzeitig bleibt das Sicherheitsniveau bei der Arbeit im Internet aufrechterhalten.

Durch Aufheben der Zeitbeschränkung für die Zwischenspeicherung des Web-Datenverkehrs wird die Effektivität der Antiviren-Untersuchung erhöht. Gleichzeitig kommt es aber zu einer verzögerten Objektbereitstellung.

➡ *Gehen Sie folgendermaßen vor, um die Zeit für die Zwischenspeicherung von Fragmenten zu beschränken oder diese Beschränkung aufzuheben:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** im Block **Erweitert** das Kontrollkästchen **Cachedauer für Datenverkehr auf 1 Sek. beschränken, um Untersuchung zu optimieren**.

ZUGRIFF AUF REGIONALE DOMAINS KONTROLLIEREN

Bei aktiviertem Geo-Filter kann Web-Anti-Virus nach Ihrer Vorgabe den Zugriff auf Webseiten je nach ihrer Zugehörigkeit zu regionalen Internet-Domains verbieten oder erlauben. Dadurch lässt sich beispielsweise der Zugriff auf Webseiten verbieten, die regionalen Domains mit einem hohem Kontaminationsgrad angehören.

Gehen Sie folgendermaßen vor, um den Zugriff auf Webseiten, die bestimmten regionalen Domains angehören, zu erlauben oder zu verbieten:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Geo-Filter** das Kontrollkästchen **Filterung nach regionalen Domains aktivieren** und geben Sie darunter in der Liste der kontrollierten Domains an, auf welche Domains der Zugriff erlaubt oder verboten werden soll, und für welche Domains das Programm mit Hilfe einer Meldung um Zugriffserlaubnis fragen soll (s. Abschnitt "Erlaubnisanfrage für den Zugriff auf eine Webseite aus einer regionalen Domain" auf S. 208).

   Für regionale Domains, die Ihrem Standort entsprechen, ist der Zugriff standardmäßig erlaubt. Für alle übrigen Domains ist standardmäßig eine Anfrage auf Zugriffserlaubnis vorgesehen.

ZUGRIFF AUF ONLINE-BANKING-DIENSTE KONTROLLIEREN

Beim Online-Banking benötigt Ihr Computer einen besonderen Schutz, da ein Verlust sensibler Daten in diesem Fall zu finanziellen Nachteilen führen kann. Web-Anti-Virus kann den Zugriff aufs Internet-Banking kontrollieren und dessen sichere Nutzung gewährleisten (s. Abschnitt "Sicherer Browser" auf S. 149). Web-Anti-Virus ermittelt automatisch, welche Internetressourcen zu Online-Banking-Diensten gehören. Damit eine Internetressource garantiert als Online-Banking-Dienst identifiziert wird, können Sie ihre Adresse einer Liste für Bank-Webseiten hinzufügen.

Gehen Sie folgendermaßen vor, um die Zugriffskontrolle für Online-Banking-Dienste anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Online-Banking** das Kontrollkästchen **Kontrolle aktivieren**. Bei der Erstinstallation wird Ihnen vorgeschlagen, den Zertifikatsinstallations-Assistenten zu starten, mit dem Sie das Kaspersky-Lab-Zertifikat für die Untersuchung von geschützten Verbindungen installieren können.

5. Erstellen Sie bei Bedarf eine Liste der Ressourcen, die Kaspersky Internet Security als Online-Banking-Dienste identifizieren soll.

LISTE MIT VERTRAUENSWÜRDIGEN ADRESSEN ERSTELLEN

Web-Anti-Virus untersucht den Datenverkehr von vertrauenswürdigen Adressen nicht auf gefährliche Objekte.

➡ *Gehen Sie folgendermaßen vor, um eine Liste mit vertrauenswürdigen Adressen anzulegen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Web-Anti-Virus**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Web-Anti-Virus** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Vertrauenswürdige Adressen** das Kontrollkästchen **Web-Datenverkehr von vertrauenswürdigen Webadressen nicht untersuchen**.
5. Erstellen Sie eine Liste der Websites / Webseiten, deren Inhalt Sie vertrauen. Gehen Sie dazu folgendermaßen vor:

   a. Klicken Sie auf **Hinzufügen**.

      Das Fenster **Adressmaske (URL)** wird geöffnet.

   b. Tragen Sie die Adresse einer Website / Webseite oder die Maske einer Website / Webseite ein.

   c. Klicken Sie auf **OK**.

      Der neue Eintrag erscheint in der Liste der vertrauenswürdigen Webadressen.
6. Wiederholen Sie gegebenenfalls die Punkte a) bis c).

IM-ANTI-VIRUS

IM-Anti-Virus untersucht den Datenverkehr, der mit Programmen zum Sofortaustausch von Nachrichten (so genannte *Instant Messenger*) übertragen wird.

Nachrichten, die mit Instant Messengern übertragen werden, können Links zu Webseiten enthalten, die verdächtig sind oder die von Angreifern für Phishing-Angriffe verwendet werden. Schädliche Programme verwenden Instant Messenger zum Senden von Spam-Nachrichten. Außerdem können Sofortnachrichten Links zu Programmen (oder sogar Programme) enthalten, die Nummern und Kennwörter von Benutzern stehlen.

Kaspersky Internet Security gewährleistet Sicherheit bei der Arbeit mit einer Vielzahl von Programmen, die dem Sofortaustausch von Nachrichten dienen. Dazu zählen ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent und IRC.

Manche Instant Messenger wie z.B. Yahoo! Messenger und Google Talk verwenden eine geschützte Verbindung. Um den Datenverkehr dieser Programme zu untersuchen, muss die Untersuchung von geschützten Verbindungen aktiviert werden (s. S. 123).

IM-Anti-Virus fängt die Nachrichten ab und untersucht sie auf gefährliche Objekte und Links. Sie können die Nachrichtentypen wählen, die untersucht werden sollen, und unterschiedliche Untersuchungsmethoden einsetzen.

Wenn IM-Anti-Virus in einer Nachricht eine Bedrohung findet, wird die Nachricht durch eine Warnung für den Benutzer ersetzt.

Dateien, die über einen Instant Messenger übertragen werden, werden von der Komponente Datei-Anti-Virus (auf S. 81) untersucht, wenn versucht wird sie zu speichern.

IN DIESEM ABSCHNITT

IM-ANTI-VIRUS AKTIVIEREN UND DEAKTIVIEREN

IM-Anti-Virus ist standardmäßig aktiviert und arbeitet im optimalen Modus. Bei Bedarf können Sie IM-Anti-Virus deaktivieren.

➡ *Gehen Sie folgendermaßen vor, um IM-Anti-Virus zu deaktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **IM-Anti-Virus aktivieren**.

SCHUTZBEREICH FÜR IM-ANTI-VIRUS FESTLEGEN

Unter Schutzbereich wird der Typ der Nachrichten verstanden, die untersucht werden sollen. Standardmäßig untersucht Kaspersky Internet Security sowohl eingehende, als auch ausgehende Nachrichten. Wenn Sie sicher sind, dass die von Ihnen gesendeten Nachrichten keine gefährlichen Objekte enthalten, können Sie die Untersuchung des ausgehenden Datenverkehrs deaktivieren.

➡ *Gehen Sie folgendermaßen vor, um die Untersuchung ausgehender Nachrichten zu deaktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.
3. Wählen Sie auf der rechten Fensterseite im Block **Schutzbereich** die Variante **Nur eingehende Nachrichten**.

LINKS IN INSTANT MESSENGER-NACHRICHTEN UNTERSUCHEN

➡ *Gehen Sie folgendermaßen vor, damit Nachrichten auf verdächtige Links und Phishing-Links untersucht werden:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.
3. Aktivieren Sie im rechten Fensterbereich unter **Untersuchungsmethoden** die Kontrollkästchen **Links mit Datenbank für verdächtige Webadressen untersuchen** und **Links mit Datenbank für Phishing-Webadressen untersuchen**.

HEURISTISCHE ANALYSE BEI DER AUSFÜHRUNG VON IM-ANTI-VIRUS VERWENDEN

Um die Effektivität des Schutzes zu steigern, können Sie eine *heuristische Analyse* verwenden (Analyse der Aktivität, die ein Objekt im System zeigt). Diese Analyse erlaubt die Erkennung neuer Schadobjekte, über die noch keine Datenbankeinträge vorliegen.

Bei der heuristischen Analyse werden alle Skripte, die in Instant Messenger-Nachrichten enthalten sind, in einer geschützten Umgebung ausgeführt. Wenn die erkannte Aktivität eines Skripte als typisch für schädliche Objekte gilt, lässt sich das Objekt mit hoher Wahrscheinlichkeit als schädlich oder verdächtig einstufen. In der Grundeinstellung ist die heuristische Analyse aktiviert.

Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **IM-Anti-Virus**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Untersuchungsmethoden** das Kontrollkästchen **Heuristische Analyse** und stellen Sie darunter das Genauigkeitsniveau ein.

PROAKTIVER SCHUTZ

Der Proaktive Schutz bietet dem Computer Schutz vor neuen Bedrohungen, über die noch keine Informationen in den Datenbanken von Kaspersky Internet Security vorhanden sind.

Der Proaktive Schutz basiert auf der Verwendung von präventiven Technologien. Mit Hilfe von Präventivtechnologien kann eine neue Bedrohung neutralisiert werden, bevor sie auf Ihrem Computer Schaden verursachen kann. Im Unterschied zu reaktiven Technologien, bei denen die Analyse Datenbankeinträgen von Kaspersky Internet Security beruht, identifizieren Präventivtechnologien eine neue Bedrohung auf Ihrem Computer aufgrund von Aktionsfolgen, die ein Programm ausführt. Wenn aufgrund der Aktivitätsanalyse die Aktionsfolge eines Programms als verdächtig eingestuft wird, sperrt Kaspersky Internet Security seine Aktivität.

Wenn beispielsweise Aktionen erkannt werden, bei denen sich ein Programm selbst in eine Netzwerkressource, in den Autostart-Ordner und in die Systemregistrierung kopiert, so handelt es sich mit hoher Wahrscheinlichkeit um einen Wurm.

Als gefährliche Aktionsfolgen gelten auch Änderungsversuche der HOSTS-Datei, versteckte Treiberinstallation u.a. Sie können die Kontrolle für eine bestimmte gefährliche Aktivität deaktivieren (s. S. 104) oder die entsprechenden Kontrollregeln ändern (s. S. 105).

Im Unterschied zur Komponente Programmkontrolle (auf S. 107) reagiert der Proaktive Schutz genau auf bestimmte Aktionsfolgen eines Programms. Die Aktivitätsanalyse erstreckt sich auf alle Programme, die auf dem Computer laufen, einschließlich der Programme, die von der Schutzkomponente Programmkontrolle der Gruppe **Vertrauenswürdig** zugeordnet wurden.

Sie können für den proaktiven Schutz eine Gruppe mit vertrauenswürdigen Programmen anlegen (s. S. 104). Über die Aktivität solcher Programme werden keine Meldungen angezeigt.

Wenn ein Computer mit den Betriebssystemen Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 oder Microsoft Windows 7 x64 arbeitet, werden nicht alle Ereignisse kontrolliert. Dies hängt mit Besonderheiten der genannten Betriebssysteme zusammen. Nicht in vollem Umfang kontrolliert werden beispielsweise das Senden von Daten über vertrauenswürdige Programme und verdächtige Aktivität im System.

IN DIESEM ABSCHNITT

PROAKTIVEN SCHUTZ AKTIVIEREN UND DEAKTIVIEREN

Der Proaktive Schutz ist standardmäßig aktiviert und arbeitet in dem Modus, der von Kaspersky Lab empfohlen wird. Sie können den Proaktiven Schutz bei Bedarf deaktivieren.

Gehen Sie folgendermaßen vor, um den Proaktiven Schutz zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Proaktiven Schutz aktivieren**.

GRUPPE MIT VERTRAUENSWÜRDIGEN PROGRAMMEN ERSTELLEN

Programme, die von der Komponente Programmkontrolle den Status **Vertrauenswürdig** erhalten, stellen keine Gefahr für das System dar. Trotzdem wird ihre Aktivität von der Komponente Proaktiver Schutz kontrolliert.

Sie können eine Gruppe mit vertrauenswürdigen Programmen erstellen, deren Aktivität nicht vom Proaktiven Schutz überwacht werden soll. Als vertrauenswürdig gelten standardmäßig Programme, die eine verifizierte digitale Signatur besitzen, und Programme, die laut der Datenbank des Kaspersky Security Network als vertrauenswürdig gelten.

Gehen Sie folgendermaßen vor, um die Einstellungen anzupassen, die für das Anlegen einer Gruppe der vertrauenswürdigen Programme gelten:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.
3. Gehen Sie im rechten Fensterbereich unter **Vertrauenswürdige Programme** folgendermaßen vor:
   - Aktivieren Sie das Kontrollkästchen **Mit digitaler Signatur**, wenn Programme, die eine verifizierte digitale Signatur besitzen, in die Gruppe der vertrauenswürdigen Programme aufgenommen werden sollen.
   - Aktivieren Sie das Kontrollkästchen **Vertrauenswürdig laut Datenbank des Kaspersky Security Network**, wenn Programme, die laut der Datenbank des Kaspersky Security Network als vertrauenswürdig gelten, in die Gruppe der vertrauenswürdigen Programme aufgenommen werden sollen.

LISTE DER GEFÄHRLICHEN AKTIVITÄT VERWENDEN

Die Liste der Aktionen, die als gefährliche Aktivität gelten, kann nicht geändert werden. Allerdings kann die Kontrolle für bestimmte gefährliche Aktivitätstypen deaktiviert werden.

Gehen Sie folgendermaßen vor, um die Kontrolle bestimmter Typen gefährlicher Aktivität zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Deaktivieren Sie im folgenden Fenster **Proaktiver Schutz** das Kontrollkästchen neben dem Namen des Aktivitätstyps, der nicht kontrolliert werden soll.

AKTION FÜR GEFÄHRLICHE PROGRAMMAKTIVITÄT ÄNDERN

Die Liste der Aktionen, die als gefährliche Aktivität gelten, kann nicht geändert werden. Geändert werden kann aber die Aktion, die Kaspersky Internet Security beim Fund einer gefährlichen Programmaktivität ausführen soll.

Gehen Sie folgendermaßen vor, um die Aktion für gefährliche Programmaktivität zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite unter **Schutz-Center** die Komponente **Proaktiver Schutz**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster **Proaktiver Schutz** in der Spalte **Ereignis** das Ereignis, für das die Regel geändert werden soll.

5. Legen Sie für das gewählte Ereignis mit Hilfe der Links im Block **Regelbeschreibung** die entsprechenden Einstellungen fest. Beispielsweise:

   a. Klicken Sie auf den Link mit der geltenden Aktion und wählen Sie im folgenden Fenster **Aktion wählen** die entsprechende Aktion.

   b. Klicken Sie auf den Link **Ein / Aus**, um festzulegen, ob die ausgeführte Operation protokolliert werden soll.

AKTIVITÄTSMONITOR

Der Aktivitätsmonitor sammelt Daten über die Aktionen der Programme auf Ihrem Computer und versorgt die anderen Schutzkomponenten mit entsprechenden Informationen, um die Effektivität des Schutzes zu steigern.

Aufgrund der Informationen, die der Aktivitätsmonitor gesammelt hat, kann Kaspersky Internet Security ein Rollback von Malware-Aktionen ausführen.

Ein Rollback von Malware-Aktionen kann von folgenden Schutzkomponenten initiiert werden:

- Durch den Aktivitätsmonitor auf Basis von Vorlagen für gefährliches Verhalten
- Vom Proaktiven Schutz
- Von Datei-Anti-Virus
- Bei einer Virenuntersuchung

Werden im System verdächtige Ereignisse gefunden, so können die Schutzkomponenten von Kaspersky Internet Security zusätzliche Informationen vom Aktivitätsmonitor anfordern. Im interaktiven Schutzmodus von Kaspersky Internet Security (s. Abschnitt "Schutzmodus auswählen" auf S. 68) stehen die Daten, die von der Komponente Aktivitätsmonitor gesammelt wurden, in einem Bericht über den Verlauf der gefährlichen Aktivität zur Verfügung. Diese Daten dienen bei der Aktionsauswahl im Meldungsfenster als Entscheidungshilfe. Wenn die Komponente ein potenziell gefährliches Programm findet, erscheint im Meldungsfenster (s. S. 209) mit der Aktionsanfrage oben ein Link, der zu einem Bericht des Aktivitätsmonitors führt.

IN DIESEM ABSCHNITT

AKTIVITÄTSMONITOR AKTIVIEREN UND DEAKTIVIEREN

Der Aktivitätsmonitor ist standardmäßig aktiviert und arbeitet in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie den Aktivitätsmonitor deaktivieren.

Es wird davor gewarnt, die Komponente auszuschalten, wenn es nicht unbedingt erforderlich ist, da hierdurch die Effektivität des Proaktiven Schutzes eingeschränkt wird. Außerdem können auch andere Schutzkomponenten beeinträchtigt werden, die von Daten abhängig sind, die der Aktivitätsmonitor sammelt, um gefundene potenzielle Bedrohungen besser zu beurteilen.

Gehen Sie folgendermaßen vor, um die Aktivitätsmonitor zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Aktivitätsmonitor**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Aktivitätsmonitor aktivieren**.

VORLAGEN FÜR GEFÄHRLICHES VERHALTEN VERWENDEN (BSS)

Vorlagen für gefährliches Programmverhalten (BSS – Behavior Stream Signatures) enthalten Aktionsfolgen für Programme, die als gefährlich klassifiziert wurden. Wenn die Aktivität eines Programms mit einer Aktivität aus den Vorlagen für gefährliches Verhalten übereinstimmt, führt Kaspersky Internet Security eine vorgegebene Aktion aus.

Die Vorlagen für gefährliches Verhalten, die der Aktivitätsmonitor verwendet, werden beim Update der Datenbanken von Kaspersky Internet Security ergänzt, um einen aktuellen und effektiven Schutz zu garantieren.

Wenn Kaspersky Internet Security im automatischen Modus arbeitet, verschiebt der Aktivitätsmonitor ein Programm standardmäßig in die Quarantäne, wenn die Programmaktivität mit einer Vorlage für gefährliches Verhalten übereinstimmt. Im interaktiven Modus wird nach einer Aktion gefragt. Sie können eine Aktion festlegen, die ausgeführt werden soll, wenn die Aktivität eines Programms mit einer Vorlage für gefährliches Verhalten übereinstimmt.

Neben einer präzisen Übereinstimmung der Programmaktivität mit einer Vorlage für gefährliches Verhalten erkennt der Aktivitätsmonitor auch Aktionen, die partiell mit Vorlagen für gefährliches Verhalten identisch sind und aufgrund einer heuristischen Analyse als verdächtig gelten. Beim Fund einer verdächtigen Aktivität fragt der Aktivitätsmonitor den Benutzer unabhängig vom Funktionsmodus nach einer Aktion.

Gehen Sie folgendermaßen vor, um die Aktion für eine Übereinstimmung von Programmaktivität und Vorlage für gefährliches Verhalten zu wählen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Aktivitätsmonitor**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Heuristische Analyse** das Kontrollkästchen **Aktualisierbare Vorlagen für gefährliches Verhalten verwenden**.
4. Wählen Sie die Option **Aktion ausführen** aus und dann, in der Dropdown-Liste, die gewünschte Aktion.

ROLLBACK VON AKTIONEN EINES SCHÄDLICHEN PROGRAMMS

Sie können eine Option verwenden, mit der die Aktionen schädlicher Programm im System rückgängig gemacht werden können. Der Aktivitätsmonitor speichert einen Verlauf der Programmaktivität, um bei Bedarf ein Rollback zu ermöglichen. Die Datenmenge, die vom Aktivitätsmonitor für ein Rollback gespeichert werden soll, kann beschränkt werden

Standardmäßig erfolgt bei der Arbeit mit Kaspersky Internet Security im Automatikmodus bei Erkennung einer schädlichen Aktivität durch die Schutzkomponenten ein automatisches Rollback. Im interaktiven Modus fragt der Aktivitätsmonitor nach einer Aktion. Sie können eine Aktion angeben, die ausgeführt werden soll, wenn erkannt wird, dass ein Rollback von Malware-Aktionen möglich ist.

Das Rollback der Aktionen schädlicher Programme betrifft lediglich ganz bestimmte Daten. Es hat keinerlei negativen Einfluss auf die Funktion des Betriebssystems und führt nicht zu Datenverlust auf Ihrem Computer.

Gehen Sie folgendermaßen vor, um festzulegen, welche Aktion erfolgen soll, wenn ein Rollback von Malware-Aktionen möglich ist:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Aktivitätsmonitor**.
3. Wählen Sie im rechten Fensterbereich unter **Rollback von Malware-Aktionen** die Variante **Aktion ausführen**. Wählen Sie dann in der Dropdown-Liste die erforderliche Aktion.

Gehen Sie folgendermaßen vor, um die Datenmenge zu beschränken, die vom Aktivitätsmonitor für ein Rollback gespeichert werden soll:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Aktivitätsmonitor**.
3. Aktivieren Sie im rechten Fensterbereich unter **Rollback von Malware-Aktionen** das Kontrollkästchen **Für ein Rollback zu speichernde Datenmenge beschränken** und legen Sie eine maximale Datenmenge fest, die der Aktivitätsmonitor für ein Rollback speichern soll.

PROGRAMMKONTROLLE

Die Programmkontrolle hindert Programme daran, systemgefährliche Aktionen auszuführen, und kontrolliert den Zugriff auf Betriebssystemressourcen und auf Ihre persönlichen Daten.

Die Komponente verfolgt die Aktionen, die von auf dem Computer installierten Programmen im System ausgeführt werden, und reguliert ihre Aktivität entsprechend den Regeln der Programmkontrolle. Diese Regeln regulieren eine potenziell gefährliche Aktivität. Dazu zählt auch der Zugriff von Programmen auf geschützte Ressourcen (beispielsweise Dateien, Ordner, Registrierungsschlüssel und Netzwerkadressen).

Die Netzwerkaktivität von Programmen wird von der Komponente Firewall kontrolliert (auf S. 116).

Wenn ein Programm zum ersten Mal auf dem Computer gestartet wird, untersucht die Komponente Programmkontrolle seine Sicherheit und verschiebt das Programm in eine der Gruppen. Eine Gruppe bestimmt die Regeln, die Kaspersky Internet Security zur Aktivitätskontrolle dieses Programms verwendet. Die Regeln der Programmkontrolle bestehen aus einer Auswahl von Rechten für den Zugriff auf Computerressourcen und von Beschränkungen für unterschiedliche Programmaktionen auf dem Computer.

Sie können die Bedingungen für die Zuordnung von Programmen zu den einzelnen Gruppen anpassen (s. S. 108), ein Programm in eine andere Gruppe verschieben (s. S. 109), und die Regeln für Kaspersky Internet Security ändern (s. S. 110).

Es wird empfohlen, am Kaspersky Security Network teilzunehmen (s. Abschnitt "Kaspersky Security Network" auf S. 184), um die Optimierung der Programmkontrolle zu unterstützen. Die Daten, die mit Hilfe des Kaspersky Security Network ermittelt werden, erlauben es, Programme genauer zu einer bestimmten Sicherheitsgruppe zuzuordnen und optimale Regeln zur Programmkontrolle zu verwenden .

Beim wiederholten Start eines Programms kontrolliert die Programmkontrolle seine Integrität. Wenn ein Programm nicht verändert wurde, wendet die Komponente die aktuellen Regeln darauf an. Wenn ein Programm verändert wurde, überprüft die Programmkontrolle es erneut wie beim ersten Start.

Um den Zugriff von Programmen auf unterschiedliche Ressourcen des Computers zu kontrollieren, können Sie die vorgegebene Liste für geschützte Ressourcen verwenden oder die Liste durch benutzerdefinierte Ressourcen erweitern (s. S. 114).

IN DIESEM ABSCHNITT

PROGRAMMKONTROLLE AKTIVIEREN UND DEAKTIVIEREN

Die Programmkontrolle ist standardmäßig aktiviert und arbeitet in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie die Programmkontrolle deaktivieren.

Gehen Sie folgendermaßen vor, um die Programmkontrolle zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Programmkontrolle aktivieren**.

PROGRAMME ZU GRUPPEN ZUORDNEN

Wenn ein Programm zum ersten Mal auf dem Computer gestartet wird, untersucht die Komponente Programmkontrolle seine Sicherheit und verschiebt das Programm in eine der Gruppen.

Programme, die keine Gefahr für das System darstellen, werden in die Gruppe **Vertrauenswürdig** verschoben. In diese Gruppe werden standardmäßig solche Programme verschoben, die eine digitale Signatur besitzen oder deren übergeordnetes Objekt eine digitale Signatur besitzt. Sie können das automatische Verschieben von Programmen mit einer digitalen Signatur in die Gruppe **Vertrauenswürdig** deaktivieren.

Das Verhalten von Programmen, die von der Programmkontrolle in die Gruppe **Vertrauenswürdig** verschoben werden, wird trotzdem von der Komponente Proaktiver Schutz kontrolliert (auf S. 103)

Um die entsprechenden Gruppen für unbekannte Programme zu ermitteln (Programme, die nicht in der Datenbank von Kaspersky Security Network enthalten sind und keine digitale Signatur besitzen), verwendet Kaspersky Internet Security standardmäßig eine heuristische Analyse. Bei dieser Analyse erfolgt eine Risikobewertung des Programms, auf deren Basis das Programm in eine bestimmte Gruppe verschoben wird. Anstelle einer heuristischen Analyse können Sie eine Gruppe festlegen, in die Kaspersky Internet Security alle unbekannten Programme automatisch verschieben soll.

Die Programmkontrolle untersucht ein Programm standardmäßig im Verlauf von 30 Sekunden. Wenn die Risikobewertung innerhalb dieses Zeitraums nicht abgeschlossen wurde, wird das Programm in die Gruppe **Schwach beschränkt** verschoben und die Risikobewertung wird im Hintergrundmodus fortgesetzt. Anschließend wird das Programm endgültig in eine Gruppe verschoben. Sie können die Dauer ändern, für die gestartete Programme untersucht

werden sollen. Wenn Sie sicher sind, dass alle Programme, die auf Ihrem Computer gestartet werden, sicher sind, können Sie die für die Untersuchung vorgesehene Dauer verringern. Sollten Sie riskante Software auf dem Computer installieren, so wird empfohlen, die Untersuchungsdauer zu erhöhen.

Wenn sich ein hoher Risikowert ergibt, werden Sie von Kaspersky Internet Security darüber informiert und Sie können eine Gruppe wählen, der das Programm zugeordnet werden soll. Die Meldung (s. S. 206) enthält eine Statistik über die Verwendung dieses Programms durch die Teilnehmer von Kaspersky Security Network. Diese Statistik und ein Verlauf über die Aktivitäten des Programms auf Ihrem Computer unterstützen Sie bei einer möglichst objektiven Entscheidung darüber, in welche Gruppe das Programm verschoben werden soll (s. Abschnitt "Interpretation von Daten über die Verwendung eines Programms durch die KSN-Teilnehmer" auf S. 115).

➡ *Gehen Sie folgendermaßen vor, um die Zuordnung von Programmen zu den einzelnen Gruppen anzupassen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Gehen Sie im rechten Fensterbereich unter **Begrenzungen festlegen** folgendermaßen vor:
   a. Aktivieren Sie das Kontrollkästchen **Programmen mit digitaler Signatur vertrauen**, damit Programme mit einer digitalen Signatur automatisch in die Gruppe **Vertrauenswürdig** verschoben werden.
   b. Legen Sie fest, auf welche Weise die Gruppen für unbekannte Programme ermittelt werden sollen:
      - Wählen Sie die Variante **Zur Ermittlung einer Gruppe die heuristische Analyse verwenden**, damit die heuristische Analyse verwendet wird, um unbekannte Programme auf die entsprechenden Gruppen zu verteilen.
      - Wählen Sie die Variante **Automatisch verschieben in die Gruppe** und wählen Sie in der Dropdown-Liste die erforderliche Gruppe aus, damit alle unbekannten Programme in eine bestimmte Gruppe verschoben werden.
   c. Geben Sie im Feld **Maximale Dauer für die Ermittlung einer Programmgruppe** an, wie lang die Ermittlung für ein gestartetes Programm dauern darf.

AKTIVITÄT VON PROGRAMMEN ANZEIGEN

Es können Informationen über auf Ihrem Computer verwendete Programme und über laufende Prozesse angezeigt werden.

➡ *Gehen Sie folgendermaßen vor, um eine Übersicht über die Programmaktivität anzuzeigen:*

1. Öffnen Sie das Programmhauptfenster (s. S. 35).
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Programmaktivität**.
3. Wählen Sie im folgenden Fenster **Programmaktivität** links oben in der Dropdown-Liste die entsprechende Programmkategorie aus.

GRUPPE ÄNDERN UND STANDARDGRUPPE WIEDERHERSTELLEN

Wenn ein Programm zum ersten Mal gestartet wird, verschiebt Kaspersky Internet Security das Programm automatisch in die entsprechende Gruppe (s. Abschnitt "Programme zu Sicherheitsgruppen zuordnen" auf S. 108). Sie können ein Programm manuell in eine andere Gruppe verschieben. Sie können ein Programm jederzeit wieder der standardmäßig vorgegebenen Gruppe zuweisen..

Die Kaspersky-Lab-Experten warnen davor, Programme aus den Gruppen, denen sie automatisch zugewiesen wurden, in andere Gruppen zu verschieben. Ändern Sie stattdessen bei Bedarf die Regeln für ein bestimmtes Programm.

➡ *Gehen Sie folgendermaßen vor, um ein Programm in eine andere Gruppe zu verschieben:*

1. Öffnen Sie das Programmhauptfenster (s. S. 35).
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Programmaktivität**.
3. Wählen Sie im folgenden Fenster **Programmaktivität** links oben in der Dropdown-Liste die entsprechende Programmkategorie aus.
4. Öffnen Sie durch Rechtsklick das Kontextmenü für das betreffende Programm und wählen Sie dort den Punkt **Verschieben in Gruppe** → **<Name der Gruppe>**.

➡ *Gehen Sie folgendermaßen vor, um ein Programm in die Standardgruppe zurückzuverschieben:*

1. Öffnen Sie das Programmhauptfenster (s. S. 35).
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Programmaktivität**.
3. Wählen Sie im folgenden Fenster **Programmaktivität** links oben in der Dropdown-Liste die entsprechende Programmkategorie aus.
4. Öffnen Sie durch Rechtsklick das Kontextmenü für das betreffende Programm und wählen Sie den Punkt **Standardgruppe wiederherstellen** → **<Name der Gruppe>**.

ARBEIT MIT DEN REGELN DER PROGRAMMKONTROLLE

Die Regeln der Programmkontrolle bestehen aus einer Auswahl von Rechten für den Zugriff auf Computerressourcen und von Beschränkungen für unterschiedliche Programmaktionen auf dem Computer.

In der Grundeinstellung werden für die Programmkontrolle die Regeln jener Gruppe verwendet, in die ein Programm bei seinem ersten Start von Kaspersky Internet Security verschoben wurde. Die Gruppenregeln wurden von Kaspersky-Lab-Experten erarbeitet, um eine optimale Kontrolle der Programmaktivität zu gewährleisten. Bei Bedarf können Sie diese Regeln ändern oder sie für ein bestimmtes Programm anpassen. Regeln für ein Programm besitzen eine höhere Priorität als Regeln für eine Gruppe.

IN DIESEM ABSCHNITT

GRUPPENREGELN ÄNDERN

In der Grundeinstellung sind für die einzelnen Gruppen optimale Rechte für den Zugriff auf Computerressourcen vorgegeben. Sie können die vordefinierten Gruppenregeln ändern.

➡ *Gehen Sie folgendermaßen vor, um Gruppenregeln zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.

3. Klicken Sie im rechten Fensterbereich unter **Anpassen der Rechte für Programme, Schutz für persönliche Daten und andere Ressourcen** auf **Programme**.
4. Wählen Sie im folgenden Fenster **Programme** die betreffende Gruppe aus der Liste und klicken Sie auf **Ändern**.
5. Wählen Sie im folgenden Fenster **Regeln für die Gruppe** die Registerkarte, die der betreffenden Ressourcenkategorie entspricht (**Dateien, Systemregistrierung** oder **Rechte**).
6. Öffnen Sie durch Rechtsklick in der Spalte der entsprechenden Aktion das Kontextmenü für die entsprechende Ressource und wählen Sie dort den entsprechenden Wert (**Erlauben**, **Verbieten** oder **Aktion erfragen**).

PROGRAMMREGELN ÄNDERN

Sie können die Begrenzungen für ein einzelnes Programm ändern oder mehrere Aktionen aus Programmregeln ausschließen. Kaspersky Internet Security kontrolliert die Aktionen nicht, die als Ausnahmen für Programmregeln hinzugefügt wurden.

Alle Ausnahmen, die in den Regeln für Programme erstellt wurden, stehen im Programmkonfigurationsfenster (s. Abschnitt"Programmkonfigurationsfenster" auf S. 38) im Abschnitt **Gefahren und Ausnahmen** zur Verfügung.

Außerdem können Sie die Verwendung von Gruppenregeln für die Zugriffskontrolle auf bestimmte Kategorien der geschützten Ressourcen deaktivieren. Der Zugriff des Programms auf diese Ressourcen wird dann durch die Regeln für das Programm gesteuert.

Gehen Sie folgendermaßen vor, um eine Regel für ein Programm zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie im rechten Fensterbereich unter **Anpassen der Rechte für Programme, Schutz für persönliche Daten und andere Ressourcen** auf **Programme**.
4. Wählen Sie im folgenden Fenster **Programme** das betreffende Programm aus der Liste und klicken Sie auf **Ändern**.
5. Öffnen Sie im folgenden Fenster **Regeln für das Programm** die Registerkarte, die der erforderlichen Ressourcenkategorie entspricht (**Dateien, Systemregistrierung** oder **Rechte**).
6. Öffnen Sie durch Rechtsklick in der Spalte der entsprechenden Aktion das Kontextmenü für die entsprechende Ressource und wählen Sie dort den entsprechenden Wert (**Erlauben**, **Verbieten** oder **Aktion erfragen**).

Gehen Sie folgendermaßen vor, um die Verwendung von Gruppenregeln für den Zugriff auf Ressourcen zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie im rechten Fensterbereich unter **Anpassen der Rechte für Programme, Schutz für persönliche Daten und andere Ressourcen** auf **Programme**.
4. Wählen Sie im folgenden Fenster **Programme** das erforderliche Programm aus der Dropdown-Liste aus.
5. Klicken Sie auf **Ändern**.
6. Öffnen Sie im folgenden Fenster **Regeln für das Programm** die Registerkarte, die der erforderlichen Ressourcenkategorie entspricht (**Dateien, Systemregistrierung** oder **Rechte**).

7. Öffnen Sie durch Rechtsklick in der Spalte der entsprechenden Aktion das Kontextmenü für die entsprechende Ressource und wählen Sie dort den Punkt **Erben**, für den das Kontrollkästchen aktiviert ist.

➡ *Gehen Sie folgendermaßen vor, um eine Ausnahme zu Programmregeln hinzuzufügen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie im rechten Fensterbereich unter **Anpassen der Rechte für Programme, Schutz für persönliche Daten und andere Ressourcen** auf **Programme**.
4. Wählen Sie im folgenden Fenster **Programme** das betreffende Programm aus der Liste und klicken Sie auf **Ändern**.
5. Wählen Sie im folgenden Fenster **Programmregeln** die Registerkarte **Ausnahmen.**
6. Aktivieren Sie die Kontrollkästchen für die Aktionen, die nicht kontrolliert werden sollen.

HERUNTERLADEN VON REGELN AUS DEM KASPERSKY SECURITY NETWORK DURCH DIE PROGRAMMKONTROLLE

Für Programme, die in der Datenbank von Kaspersky Security Network gefunden wurden, werden standardmäßig die aus dieser Datenbank geladenen Regeln verwendet.

Wenn ein Programm beim ersten Start nicht in der Datenbank von Kaspersky Security Network verzeichnet war, danach jedoch entsprechende Programminformationen hinzugefügt wurden, werden die Regeln für die Kontrolle dieses Programms automatisch von Kaspersky Internet Security aktualisiert.

Sie können die Verwendung von Regeln aus dem Kaspersky Security Network und (oder) die automatische Aktualisierung der Regeln für bisher unbekannte Programme deaktivieren.

➡ *Gehen Sie folgendermaßen vor, um die Verwendung von Regeln aus dem Kaspersky Security Network zu deaktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Deaktivieren Sie auf der rechten Fensterseite im Block **Begrenzungen festlegen** das Kontrollkästchen **Regeln für Programme aus dem Kaspersky Security Network (KSN) herunterladen**.

➡ *Um die Aktualisierung der Regeln aus dem Kaspersky Security Network für bisher unbekannte Programme zu deaktivieren, gehen Sie wie folgt vor:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Deaktivieren Sie auf der rechten Fensterseite im Block **Begrenzungen festlegen** das Kontrollkästchen **Regeln für bisher unbekannte Programme aus KSN aktualisieren**.

VERERBUNG VON BESCHRÄNKUNGEN EINES ÜBERGEORDNETEN PROZESSES

Programme und Prozesse können auf Ihrem Computer nicht nur von Ihnen gestartet werden, sondern auch von bereits laufenden Programmen (Prozessen), die in diesem Kontext als *übergeordnet* bezeichnet werden. Wenn ein übergeordneter Prozess weniger Rechte besitzt als ein von ihm zu startendes Programm, so wendet die

Programmkontrolle die gleichen Beschränkungen auf das Programm an, die für den übergeordneten Prozess gelten. Das zu startende Programm *erbt* also die Beschränkungen des übergeordneten Prozesses.

Dieser Mechanismus verhindert, dass vertrauenswürdige Programme von zweifelhaften Programmen oder von Programmen, die über beschränkte Rechte verfügen, dazu benutzt werden, privilegierte Aktionen auszuführen.

Wenn die Aktivität eines Programms blockiert wird, weil ein übergeordneter Prozess unzureichende Rechte besitzt, können Sie diese Rechte anpassen oder die Vererbung von Beschränkungen eines übergeordneten Prozesses deaktivieren.

Das Ändern von Rechten eines übergeordneten Prozesses oder das Ausschalten des Vererbungsmechanismus sollte nur dann erfolgen, wenn Sie absolut sicher sind, dass die Aktivität des Prozesses keine Gefahr für das System darstellt!

➡ *Gehen Sie folgendermaßen vor, um die Vererbung von Beschränkungen eines übergeordneten Prozesses zu deaktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie im rechten Fensterbereich unter **Anpassen der Rechte für Programme, Schutz für persönliche Daten und andere Ressourcen** auf **Programme**.
4. Wählen Sie im folgenden Fenster **Programme** das erforderliche Programm aus der Dropdown-Liste aus.
5. Klicken Sie auf **Ändern**.
6. Wählen Sie im folgenden Fenster **Programmregeln** die Registerkarte **Ausnahmen**.
7. Aktivieren Sie dann das Kontrollkästchen **Beschränkungen des übergeordneten Prozesses (Programms) nicht übernehmen**.

REGELN FÜR NICHT VERWENDETE PROGRAMME LÖSCHEN

Standardmäßig werden die Regeln für Programme, die innerhalb der letzten 60 Tage nicht gestartet wurden, automatisch gelöscht. Sie können die Speicherdauer der Regeln für nicht verwendete Programme ändern oder das automatische Löschen deaktivieren.

➡ *Gehen Sie folgendermaßen vor, um die Speicherdauer für Programmregeln zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Erweitert** das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit** und geben Sie die entsprechende Anzahl der Tage an.

➡ *Gehen Sie folgendermaßen vor, um das automatische Löschen der Regeln für nicht verwendete Programme zu deaktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Deaktivieren Sie im rechten Fensterbereich im Block **Erweitert** das Kontrollkästchen **Regeln für Programme löschen, wenn nicht gestartet seit**.

SCHUTZ FÜR BETRIEBSSYSTEMRESSOURCEN UND PERSÖNLICHE DATEN

Die Programmkontrolle verwaltet die Rechte von Programmen, die für das Ausführen von Aktionen mit diversen Ressourcenkategorien des Betriebssystems und der persönlichen Daten gelten.

Die Kaspersky-Lab-Experten haben Kategorien für geschützte Ressourcen vordefiniert. Diese Liste kann nicht verändert werden. Sie können dieser Liste aber benutzerdefinierte Kategorien und / oder einzelne Ressourcen hinzufügen, und die Kontrolle bestimmter Ressourcen deaktivieren.

Außerdem können Sie bestimmte Ressourcen zu den Ausnahmen hinzufügen. Der Zugriff auf solche Ressourcen wird nicht kontrolliert.

Gehen Sie folgendermaßen vor, um geschützte persönliche Daten hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie rechts im Fenster auf **Datenschutz**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Persönliche Daten** in der Dropdown-Liste die erforderliche Kategorie für persönliche Daten aus.
5. Klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie im erscheinenden Menü den gewünschten Ressourcentyp.
6. Legen Sie im folgenden Fenster **Benutzerressource** in Abhängigkeit von der hinzuzufügenden Ressource die notwendigen Parameter fest.

Gehen Sie folgendermaßen vor, um eine Kategorie für geschützte persönliche Daten zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie rechts im Fenster auf **Datenschutz**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Persönliche Daten** auf **Kategorie hinzufügen**.
5. Geben Sie im folgenden Fenster **Kategorie für Benutzerressourcen** einen Namen für die neue Ressourcenkategorie ein.

Gehen Sie folgendermaßen vor, um geschützte Parameter und Ressourcen des Betriebssystems hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie rechts im Fenster auf **Datenschutz**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Betriebssystem** in der Dropdown-Liste **Kategorie** die erforderliche Kategorie für Objekte des Betriebssystems aus.
5. Klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie im erscheinenden Menü den gewünschten Ressourcentyp aus.
6. Legen Sie im folgenden Fenster **Benutzerressource** in Abhängigkeit von der hinzuzufügenden Ressource die notwendigen Parameter fest.

Gehen Sie folgendermaßen vor, um den Ausnahmen eine Ressource hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Programmkontrolle**.
3. Klicken Sie rechts im Fenster auf **Datenschutz**.
4. Betätigen Sie im erscheinenden Fenster auf der Registerkarte **Ausnahmen** die Schaltfläche **Hinzufügen** und wählen Sie im erscheinenden Menü den gewünschten Ressourcentyp.
5. Legen Sie im folgenden Fenster **Benutzerressource** in Abhängigkeit von der hinzuzufügenden Ressource die notwendigen Parameter fest.

INTERPRETATION VON DATEN ÜBER DIE VERWENDUNG EINES PROGRAMMS DURCH DIE KSN-TEILNEHMER

Die Informationen über die Verwendung eines Programms durch die Teilnehmer an Kaspersky Security Network (s. S. 185) können helfen, eine objektive Entscheidung darüber zu fällen, welcher Status einem Programm zugewiesen werden soll, das auf Ihrem Computer gestartet wird. Um die Gefährlichkeit eines Programms auf Grundlage der Daten aus dem KSN genau beurteilen zu können, sind genauere Informationen darüber erforderlich, wie das Programm auf Ihren Computer gekommen ist.

Die Kaspersky-Lab-Experten unterscheiden folgende möglichen Quellen für das Auftreten neuer Programme auf einem Computer.

- Download aus dem Internet und anschließender Start einer Installationsdatei durch den Benutzer
- Automatischer Download und Start einer Installationsdatei, wenn der Benutzer über einen Link auf eine Webseite wechselt.
- Der Benutzer startet eine Installationsdatei, die sich auf einer CD / DVD befindet oder von dort auf die Festplatte kopiert wurde.
- Der Benutzer startet eine Installationsdatei, die sich auf einem USB-Speicher befindet oder von dort auf die Festplatte kopiert wurde.
- Der Benutzer startet eine Installationsdatei, die per E-Mail, Instant Messenger oder über ein soziales Netzwerk empfangen wurde.

Die Statistik über die Verwendung eines Programms durch die Teilnehmer von Kaspersky Security Network enthält die Verwendungshäufigkeit und -dauer für das Programm. Für die Verwendung eines Programms bestehen folgende statistische Varianten:

- **sehr selten** (weniger als 100 KSN-Teilnehmer verwenden dieses Programm) und **kürzlich** (die Datei wurde vor einigen Tagen in KSN aufgenommen).
- **selten** (weniger als 1.000 KSN-Teilnehmer) und relativ **lange** (vor einigen Monaten). Die meisten Benutzer beschränken die Aktivität dieses Programms.
- **häufig** (über 100.000 KSN-Teilnehmer) und **lange** (vor über einem halben Jahr). Die meisten Benutzer vertrauen diesem Programm.
- **häufig** (über 100.000 KSN-Teilnehmer) und **kürzlich** (vor einigen Wochen). Die meisten Benutzer vertrauen diesem Programm oder beschränken es.
- **sehr häufig** (über 100.000 KSN-Teilnehmer) und **kürzlich**. Die meisten Benutzer vertrauen diesem Programm.

NETZWERKSCHUTZ

Unterschiedliche Schutzkomponenten, Tools und Konfigurationen von Kaspersky Internet Security bieten Ihnen Sicherheit bei der Arbeit in einem Netzwerk.

Die folgenden Abschnitte informieren ausführlich über folgende Themen: Funktionsprinzipien und Einstellungen der Firewall und des Schutzes vor Netzwerkangriffen, Netzwerkmonitor, Untersuchung von geschützten Verbindungen, Proxyserver-Einstellungen, Kontrolle von Netzwerkports.

IN DIESEM ABSCHNITT

FIREWALL

Firewall gewährleistet Sicherheit bei der in lokalen Netzwerken und im Internet.

Die Komponente filtert die gesamte Netzwerkaktivität in Übereinstimmung mit den Netzwerkregeln der Programmkontrolle. Eine Netzwerkregel ist eine Aktion, die von der Firewall ausgeführt wird, wenn ein Versuch für eine Verbindung erkannt wird, die einen bestimmten Status besitzt. Jeder Netzwerkverbindung wird ein Status zugewiesen, der durch bestimmte Parameter definiert wird: Richtung und Protokoll für die Datenübertragung, Adressen und Ports, mit denen die Verbindung erfolgt.

Die Firewall analysiert die Parameter der Netzwerke, die Sie mit Ihrem Computer verbinden. Wenn das Programm im interaktiven Funktionsmodus arbeitet, fragt die Firewall Sie bei der ersten Verbindung nach dem Status des verbundenen Netzwerks (s. S. 207). Wenn der interaktive Funktionsmodus deaktiviert wurde, ermittelt die Firewall den Status, wozu Netzwerktyp, Adressenbereich und anderen Merkmale verwendet werden. Bei Bedarf können Sie den Status der Netzwerkverbindung (s. S. 117) manuell ändern.

IN DIESEM ABSCHNITT

FIREWALL AKTIVIEREN UND DEAKTIVIEREN

Die Firewall ist standardmäßig aktiviert und arbeitet in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie die Firewall deaktivieren.

Gehen Sie folgendermaßen vor, um die Firewall zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Firewall aktivieren**.

NETZWERKSTATUS ÄNDERN

Vom Status der Netzwerkverbindung hängt ab, welche Filterregeln für die Netzwerkaktivität dieser Verbindung zur Anwendung kommen. Bei Bedarf können Sie den Netzwerkstatus ändern.

Gehen Sie folgendermaßen vor, um den Status einer Netzwerkverbindung zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Wählen Sie rechts in der Liste **Netzwerke** eine Netzwerkverbindung aus und klicken Sie auf **Ändern**, um ein Fenster mit den Netzwerkeinstellungen zu öffnen.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Eigenschaften** den erforderlichen Status aus der Dropdown-Liste aus.

ARBEIT MIT DEN FIREWALL-REGELN

Die Firewall arbeitet mit zwei Arten von Regeln:

- *Paketregeln.* Dienen zur Definition von Beschränkungen für die Pakete, wobei das Programm keine Rolle spielt. Solche Regeln beziehen sich meistens auf die eingehende Netzwerkaktivität bestimmter Ports mit den Protokollen TCP und UDP und regulieren die Filterung von ICMP-Nachrichten.
- *Programmregeln*. Dienen zur Definition von Beschränkungen für die Netzwerkaktivität eines konkreten Programms. Solche Regeln erlauben es, die Aktivitätsfilterung genau anzupassen, wenn beispielsweise ein bestimmter Typ von Netzwerkverbindungen für konkrete Programme verboten, für andere aber erlaubt werden soll.

Paketregeln besitzen eine höhere Priorität als Programmregeln. Wenn für einen Typ der Netzwerkaktivität sowohl Paketregeln als auch Regeln für Programme vorhanden sind, wird diese Netzwerkaktivität nach den Paketregeln verarbeitet. Außerdem können Sie für jede Regel eine Ausführungspriorität (s. S. 119) festlegen.

PAKETREGEL ERSTELLEN

Paketregeln bestehen aus einer Kombination von Bedingungen und Aktionen, die unter bestimmten Bedingungen mit Paketen ausgeführt werden.

Wenn Sie Paketregeln erstellen, beachten Sie, dass diese eine höhere Priorität besitzen als Regeln für Programme.

Gehen Sie folgendermaßen vor, um eine neue Paketregel zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Paketregeln** auf **Hinzufügen**.
5. Legen Sie im folgenden Fenster **Netzwerkregel** die entsprechenden Parameter fest und klicken Sie auf **OK**.

6. Weisen Sie der neuen Regel eine Priorität zu. Verschieben Sie die Regel dazu mit den Schaltflächen **Aufwärts** und **Abwärts** an die entsprechende Position.

GRUPPENREGELN ÄNDERN

Analog zur Komponente Programmkontrolle (auf S. 107) verwendet die Firewall zur Filterung der Netzwerkaktivität standardmäßig die Regeln der Gruppe, in die das Programm verschoben wurde.

Die Netzwerkregeln für Gruppen legen fest, welche Rechte die Programme, die dieser Gruppe angehören, für den Zugriff auf unterschiedliche Netzwerke besitzen. Sie können die vordefinierten Netzwerkregeln einer Gruppe ändern oder neue Regeln hinzufügen.

Gehen Sie folgendermaßen vor, um eine Netzwerkregel für eine Gruppe hinzuzufügen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Programmregeln** die betreffende Gruppe aus der Liste aus und klicken Sie auf **Ändern**.
5. Wählen Sie im folgenden Fenster **Gruppenregeln** die Registerkarte **Netzwerkregeln** und klicken Sie auf **Hinzufügen**.
6. Legen Sie im folgenden Fenster **Netzwerkregel** die entsprechenden Parameter fest und klicken Sie auf **OK**.
7. Weisen Sie der neuen Regel eine Priorität zu. Verschieben Sie dazu die Regel mit den Schaltflächen **Aufwärts** und **Abwärts** an die entsprechende Position der Liste.

Gehen Sie folgendermaßen vor, um eine Netzwerkregel für eine Gruppe zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Programmregeln** die betreffende Gruppe aus der Liste aus und klicken Sie auf **Ändern**.
5. Wählen Sie im folgenden Fenster **Gruppenregeln** die Registerkarte **Netzwerkregeln**.
6. Öffnen Sie durch Rechtsklick in der Spalte **Erlaubnis** das Kontextmenü für die betreffende Regel und wählen Sie dort den entsprechenden Wert **(Erlauben**, **Verbieten** oder **Aktion erfragen**).

PROGRAMMREGELN ÄNDERN

Sie können Netzwerkregeln für bestimmte Programme erstellen. Netzwerkregeln für ein Programm besitzen eine höhere Priorität als Netzwerkregeln für eine Gruppe.

Gehen Sie folgendermaßen vor, um eine neue Netzwerkregel für ein Programm zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Wählen Sie im folgenden Fenster auf der Registerkarte **Programmregeln** ein Programm und klicken Sie auf **Ändern**, um das Konfigurationsfenster für Regeln zu öffnen.

5. Klicken Sie im folgenden Fenster **Regeln für das Programm** auf der Registerkarte **Netzwerkregeln** auf **Hinzufügen**, um das Fenster zu öffnen, in dem eine neue Netzwerkregel für das Programm erstellt wird.

6. Legen Sie im folgenden Fenster **Netzwerkregel** die entsprechenden Parameter fest und klicken Sie auf **OK**.

7. Weisen Sie der neuen Regel eine Priorität zu. Verschieben Sie dazu die Regel mit den Schaltflächen **Aufwärts** und **Abwärts** an die entsprechende Position der Liste.

PRIORITÄT EINER REGEL ÄNDERN

Die Priorität für die Ausführung einer Regel wird durch ihre Position in der Liste bestimmt. Die erste Regel in der Liste besitzt die höchste Priorität.

Jede manuell neu erstellte Paketregel wird am Ende der Liste für Paketregeln hinzugefügt.

Die Gruppen für Programme sind nach Programmnamen angeordnet und die Priorität der Regeln gilt nur für eine bestimmte Gruppe. Benutzerdefinierte Regeln für Programme besitzen eine höhere Priorität als Regeln, die Gruppenregeln erben.

➡ *Gehen Sie folgendermaßen vor, um die Priorität einer Paketregel zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Paketregeln** eine Regel und verschieben Sie sie durch Klicken auf **Aufwärts** oder **Abwärts** an die erforderliche Position der Liste.

➡ *Gehen Sie folgendermaßen vor, um die Priorität von Regeln für ein Programm oder eine Gruppe zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

4. Wählen Sie im folgenden Fenster auf der Registerkarte **Regeln für Programme** ein Programm oder eine Gruppe aus, und klicken Sie auf **Ändern**, um das Konfigurationsfenster für Regeln zu öffnen.

5. Wählen Sie im folgenden Fenster auf der Registerkarte **Netzwerkregeln** eine Regel und verschieben Sie sie durch Klicken auf **Aufwärts** oder **Abwärts** an die erforderliche Position der Liste.

BENACHRICHTIGUNGEN ÜBER VERÄNDERUNGEN EINES NETZWERKS ANPASSEN

Die Parameter von Netzwerkverbindungen können sich im Verlauf der Arbeit ändern. Sie können sich über Veränderungen der Netzwerkeinstellungen informieren lassen.

➡ *Gehen Sie folgendermaßen vor, um die Benachrichtigungen über Veränderungen der Parameter einer Netzwerkverbindung anzupassen:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.

3. Wählen Sie im rechten Fensterbereich unter **Netzwerke** eine Netzwerkverbindung aus und klicken Sie auf **Ändern**, um ein Fenster mit den Netzwerkeinstellungen zu öffnen.

4. Aktivieren Sie im folgenden Fenster auf der Registerkarte **Erweitert** im Block **Informieren** die Kontrollkästchen für Ereignisse, über die Meldungen erfolgen sollen.

ERWEITERTE EINSTELLUNGEN FÜR DIE FIREWALL

Für die Firewall sind folgende erweiterte Einstellungen verfügbar:

- Aktiven FTP-Modus zulassen.
- Verbindung blockieren, wenn keine Aktionsanfrage möglich ist (wenn das Programminterface nicht geladen ist).
- Firewall erst ausschalten, nachdem das System vollständig heruntergefahren wurde.

In der Grundeinstellung sind diese Parameter deaktiviert.

Gehen Sie folgendermaßen vor, um die Firewall zusätzlich anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Firewall**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Paketregeln** auf die Schaltfläche **Erweitert** , um die erweiterten Einstellungen zu öffnen
5. Aktivieren / deaktivieren Sie im folgenden Fenster **Erweitert** die Kontrollkästchen für die entsprechenden Parameter.

SCHUTZ VOR NETZWERKANGRIFFEN

Der Schutz vor Netzwerkangriffen überwacht den eingehenden Datenverkehr auf für Netzwerkangriffe charakteristische Aktivität. Wenn ein Angriffsversuch auf Ihren Computer erkannt wird, blockiert Kaspersky Internet Security jede Art von Netzwerkaktivität des angreifenden Computers im Hinblick auf Ihrem Computer.

In der Grundeinstellung dauert die Blockade eine Stunde. Auf dem Bildschirm erscheint eine Meldung über den Angriffsversuch. Die Meldung enthält Informationen über den angreifenden Computer. Beschreibungen der momentan bekannten Netzwerkangriffe (s. Abschnitt "Arten der erkennbaren Netzwerkangriffe" auf S. 120) und entsprechende Abwehrmethoden sind in den Datenbanken von Kaspersky Internet Security enthalten. Die Liste der Angriffe, die der Schutz vor Netzwerkangriffen erkennt, wird im Rahmen des Updates (s. Abschnitt "Update" auf S. 77) der Datenbanken aktualisiert.

IN DIESEM ABSCHNITT

ARTEN DER ERKENNBAREN NETZWERKANGRIFFE

Heutzutage existiert einen Vielzahl unterschiedlicher Arten von Netzwerkangriffen. Diese Angriffe nutzen sowohl Schwachstellen des Betriebssystems, als auch installierte System- und Anwendungsprogramme aus.

Um rechtzeitig für die Sicherheit des Computers zu sorgen, ist es wichtig zu wissen, welche Arten von Netzwerkangriffen ihm drohen können. Die bekannten Netzwerkangriffe lassen sich bedingt in drei große Gruppen unterteilen:

- *Scannen von Ports* – Diese Bedrohungsart stellt getrennt betrachtet keinen Angriff dar, sondern geht diesem voraus, weil sie eine der effektivsten Methoden ist, Informationen über einen Remote-Computer zu erhalten. Die Methode besteht darin, die von Netzwerkdiensten auf dem angegriffenen Computer verwendeten UDP/TCP-Ports zu scannen, um deren Status (geschlossene oder offene Ports) zu ermitteln.

  Das Scannen von Ports gibt Aufschluss darüber, welche Angriffstypen für ein bestimmtes System am meisten Erfolg versprechen. Außerdem verleihen die aus dem Scannen resultierenden Informationen ("Abdruck" des Systems) dem Angreifer eine Vorstellung vom Typ des Betriebssystems auf dem entfernten Computer. Dadurch lässt sich die Art der relevanten Angriffe weiter einkreisen und damit die zum Ausführen der Angriffe notwendige Zeit verkürzen. Außerdem können die für das Betriebssystem spezifischen Sicherheitslücken ausgenutzt werden.

- *DoS-Angriffe* oder Angriffe, die zur Dienstverweigerung führen Das Ziel dieser Angriffe besteht darin, die Instabilität des angegriffenen Systems hervorzurufen oder es vollständig außer Gefecht zu setzen. Aufgrund solcher Angriffe können die betroffenen Informationsressourcen unzugänglich werden (z.B. gestörter Internetzugriff).

  Es gibt zwei Haupttypen von DoS-Angriffen:

  - Es werden spezielle Pakete an den angegriffenen Computer geschickt, die dieser nicht erwartet. Die Folge ist eine Überlastung oder ein Systemabsturz.

  - An den angegriffenen Computer wird innerhalb eines kurzen Zeitraums eine große Anzahl von Paketen geschickt, die dieser Computer nicht verarbeiten kann. Als Folge erschöpfen die Systemressourcen.

  Die folgenden Angriffe bieten gute Beispiele für diese Gruppe:

  - Der Angriff *Ping of death* besteht im Senden eines ICMP-Pakets, dessen Größe den zulässigen Wert von 64 KB überschreitet. Dieser Angriff kann zum Absturz bestimmter Betriebssysteme führen.

  - Bei dem Angriff *Land* wird an einen offenen Port Ihres Computers eine Anfrage auf Verbindungsherstellung mit sich selbst gesendet. Der Angriff führt im angegriffenen Computer zu einer Endlosschleife, was eine stark erhöhte Prozessorbelastung zur Folge hat und bei bestimmten Betriebssystemen zum Absturz führen kann.

  - Bei dem Angriff *ICMP Flood* wird eine große Anzahl von ICMP-Paketen an Ihren Computer gesendet Da der Computer auf jedes eintreffende Paket reagieren muss, kommt es zu einer erheblichen Erhöhung der Prozessorauslastung.

  - Bei dem Angriff *SYN Flood* wird eine große Menge von Verbindungsanfragen an Ihren Computer gesendet. Das System reserviert für jede dieser Verbindungen bestimmte Ressourcen, wodurch es seine Ressourcen vollständig verbraucht und nicht mehr auf andere Verbindungsversuche reagiert.

- *Angriffe zur "Übernahme"* - Diese Angriffe zielen auf die "Übernahme" des Systems ab. Dies ist der gefährlichste Angriffstyp, weil das System bei erfolgreichem Angriff dem Angreifer gegenüber vollkommen wehrlos ist.

  Dieser Angriff wird benutzt, um von einem Remote-Computer vertrauliche Informationen zu stehlen (beispielsweise Kreditkartennummern und Kennwörter). Ein weiteres Ziel kann darin bestehen, sich im System einzunisten, um später die Rechnerressourcen für die Zwecke des Angreifers zu nutzen (das angegriffene System wird in einem Zombie-Netzwerk oder als "Brückenkopf" für neue Angriffe verwendet).

  Zu dieser Gruppe gehört eine große Anzahl von Angriffen. Sie lassen sich abhängig von dem Betriebssystem, das auf einem Computer installiert ist, in drei Kategorien unterteilen: Angriffe auf Microsoft Windows-Systeme, Angriffe auf Unix-Systeme und eine allgemeine Gruppe für Netzwerkdienste, die in beiden Betriebssystemen verwendet werden.

  Die meistverbreiteten Arten von Angriffen, die auf Netzwerkdienste eines Betriebssystems zugreifen, sind:

  - *Angriffe mit dem Ziel des Pufferüberlaufs*. Ein Pufferüberlauf tritt durch fehlende (oder unzureichende) Kontrolle bei der Arbeit mit Daten-Arrays auf. Dieser Typ von Schwachstellen gehört zu den ältesten und lässt sich am leichtesten von Angreifern ausnutzen.

- *Angriffe, die auf Fehlern in Formatzeilen beruhen*. Formatzeilenfehler treten auf, weil die Eingabeparameter von Formatfunktionen des Typs *printf(), fprintf(), scanf()* und anderer Standardbibliotheken der Sprache C unzureichend kontrolliert werden. Wenn diese Sicherheitslücke in einem Programm vorhanden ist, kann ein Angreifer die vollständige Kontrolle über das System übernehmen, wenn es ihm gelingt, speziell erstellte Anfragen zu senden.

  Wenn solche Schwachstellen auf dem Benutzercomputer vorhanden sind, werden sie vom Detektionssystem für Angriffe in den gebräuchlichsten Netzwerkdiensten (FTP, POP3, IMAP) automatisch analysiert und ihre Verwendung wird verhindert.

- *Angriffe, die sich auf das Betriebssystem Microsoft Windows richten,* beruhen auf der Verwendung von Sicherheitslücken der auf einem Computer installierten Software (beispielsweise solcher Programme wie Microsoft SQL Server, Microsoft Internet Explorer, Messenger, sowie Systemkomponenten, die über ein Netzwerk erreichbar sind: DCom, SMB, Wins, LSASS, IIS5).

Als weiterer häufig anzutreffender Typ von Übernahmeangriffen lässt sich die Verwendung unterschiedlicher Arten von schädlichen Skripte nennen. Dazu zählen auch Skripte, die von Microsoft Internet Explorer verarbeitet werden, sowie die Variationen des Helkern-Wurms. Bei einem Helkern-Angriff werden spezielle UDP-Pakete mit ausführbarem schädlichem Code an einen entfernten Computer gesendet.

SCHUTZ VOR NETZWERKANGRIFFEN AKTIVIEREN UND DEAKTIVIEREN

Der Schutz vor Netzwerkangriffen ist standardmäßig aktiviert und arbeitet in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie den Schutz vor Netzwerkangriffen deaktivieren.

➧ *Gehen Sie folgendermaßen vor, um den Schutz vor Netzwerkangriffen zu deaktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Schutz vor Netzwerkangriffen**.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Schutz vor Netzwerkangriffen aktivieren**.

PARAMETER FÜR DAS BLOCKIEREN ÄNDERN

In der Grundeinstellung blockiert der Schutz vor Netzwerkangriffen die Netzwerkaktivität eines angreifenden Computers für 60 Minuten. Sie können das Blockieren für einen bestimmten Computer aufheben oder die Sperrdauer ändern.

➧ *Gehen Sie folgendermaßen vor, um den Zeitraum, für den ein angreifender Computer gesperrt werden soll, zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Schutz vor Netzwerkangriffen**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Angreifenden Computer zur Sperrliste hinzufügen für** und legen Sie eine Sperrdauer fest.

➧ *Gehen Sie folgendermaßen vor, um einen angreifenden Computer freizugeben:*

1. Öffnen Sie das Programmhauptfenster (s. S. 35).
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Netzwerkmonitor**.
3. Wählen Sie im folgenden Fenster **Netzwerkmonitor** auf der Registerkarte **Blockierte Computer** einen blockierten Computer aus und klicken Sie auf **Freigeben**.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN

Eine Verbindung unter Verwendung des SSL / TLS-Protokolls bietet den Schutz des Kommunikationskanals im Internet. Das SSL / TLS-Protokoll erlaubt die Identifikation der am Datenaustausch beteiligten Partner. Dazu dienen elektronische Zertifikate. Außerdem werden die übertragenen Daten verschlüsselt und beim Übertragungsvorgang wird die Datenintegrität gewährleistet.

Diese Besonderheiten des Protokolls werden jedoch von Angreifern zur Verbreitung schädlicher Programme benutzt, da die meisten Antiviren-Produkte den SSL / TLS-Verkehr nicht untersuchen.

Kaspersky Internet Security untersucht geschützte Verbindungen mit Hilfe eines Zertifikats von Kaspersky Lab.

Wenn bei der Verbindung mit einem Server ein inkorrektes Zertifikat gefunden wird (wenn es z.B. von einem Angreifer ausgetauscht wurde), erscheint auf dem Bildschirm eine Meldung, in der Sie das Zertifikat akzeptieren oder ablehnen.

Wenn Sie sicher sind, dass die Verbindung mit einer Webseite trotz des inkorrekten Zertifikats immer ungefährlich ist, können Sie die Webseite in die Liste der vertrauenswürdigen Adressen aufnehmen. Kaspersky Internet Security wird verschlüsselte Verbindungen mit dieser Webseite danach nicht mehr untersuchen.

Sie können den Assistenten für die Zertifikatinstallation verwenden, um eine teilweise interaktive Installation des Zertifikats für die Untersuchung der geschützten Verbindungen in den Browsern Microsoft Internet Explorer, Mozilla Firefox (sofern nicht gestartet) und Google Chrome vorzunehmen und um Anweisungen zur Installation des Kaspersky-Lab-Zertifikats für den Browser Opera zu erhalten.

Gehen Sie folgendermaßen vor, um die Untersuchung von geschützten Verbindungen zu aktivieren und das Kaspersky-Lab-Zertifikat zu installieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** die Komponente **Netzwerk**.
3. Aktivieren Sie im folgenden Fenster das Kontrollkästchen **Geschützte Verbindungen untersuchen**. Bei der ersten Aktivierung dieser Einstellung wird der Assistent zur Zertifikatinstallation automatisch gestartet.
4. Klicken Sie auf die Schaltfläche **Zertifikat installieren**, wenn der Assistent nicht gestartet wurde. Es wird ein Assistent gestartet, der Sie bei der Installation des Kaspersky-Lab-Zertifikats unterstützt.

IN DIESEM ABSCHNITT

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN IN MOZILLA FIREFOX

Der Browser Mozilla Firefox verwendet nicht den Zertifikatsspeicher von Microsoft Windows. Bei der Verwendung von Firefox ist es zur Untersuchung von SSL-Verbindungen erforderlich, das Kaspersky-Lab-Zertifikat manuell zu installieren.

Sie können den Assistenten zur Zertifikatinstallation auch verwenden, wenn der Browser nicht gestartet ist.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat manuell zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.
2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.
3. Wählen Sie im Block **Zertifikate** die Registerkarte **Sicherheit** und klicken Sie auf **Zertifikate anzeigen**.
4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Aktionen, für deren Untersuchung das installierte Zertifikat verwendet werden soll. Klicken Sie zur Anzeige von Informationen zu dem Zertifikat auf **Anzeigen**.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat für Mozilla Firefox Version 3.x manuell zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.

3. Klicken Sie auf der Registerkarte **Verschlüsselung** auf **Zertifikate anzeigen**.

4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Aktivieren Sie im folgenden Fenster die Kontrollkästchen der Aktionen, für deren Untersuchung das installierte Zertifikat verwendet werden soll. Klicken Sie zur Anzeige von Informationen zu dem Zertifikat auf **Anzeigen**.

Wenn Ihr Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 arbeitet, lautet der Pfad der Zertifikatsdatei von Kaspersky Lab: *%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

UNTERSUCHUNG GESCHÜTZTER VERBINDUNGEN IN OPERA

Der Browser Opera verwendet nicht den Zertifikatsspeicher von Microsoft Windows. Bei der Verwendung von Opera ist es zur Untersuchung von SSL-Verbindungen erforderlich, das Kaspersky-Lab-Zertifikat manuell zu installieren.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.

3. Wählen Sie auf der linken Fensterseite die Registerkarte **Sicherheit** und klicken Sie auf **Zertifikate verwalten**.

4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Klicken Sie im folgenden Fenster auf **Installieren**. Das Kaspersky-Lab-Zertifikat wird installiert. Um Informationen zum Zertifikat anzuzeigen und die Aktionen, bei denen das Zertifikat verwendet werden soll, auszuwählen, wählen Sie das Zertifikat in der Liste aus und klicken Sie auf **Anzeigen**.

Gehen Sie folgendermaßen vor, um das Kaspersky-Lab-Zertifikat für Opera Version 9.x zu installieren:

1. Wählen Sie im Menü des Browsers den Punkt **Tools** → **Einstellungen**.

2. Wählen Sie im folgenden Fenster den Abschnitt **Erweitert**.

3. Wählen Sie auf der linken Fensterseite die Registerkarte **Sicherheit** und klicken Sie auf **Zertifikate verwalten**.

4. Wählen Sie im folgenden Fenster die Registerkarte **Zertifizierungsstellen** und klicken Sie auf **Importieren**.

5. Wählen Sie im folgenden Fenster die Datei des Kaspersky-Lab-Zertifikats. Pfad der Datei des Kaspersky-Lab-Zertifikats: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

6. Klicken Sie im folgenden Fenster auf **Installieren**. Das Kaspersky-Lab-Zertifikat wird installiert.

Wenn Ihr Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 arbeitet, lautet der Pfad der Zertifikatsdatei von Kaspersky Lab: *%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

NETZWERKMONITOR

Der Netzwerkmonitor dient dazu, in Echtzeit Informationen über die Netzwerkaktivität anzuzeigen.

Gehen Sie folgendermaßen vor, um Informationen über die Netzwerkaktivität anzuzeigen:

1. Öffnen Sie das Programmhauptfenster (s. S. 35).

2. Wählen Sie im unteren Fensterbereich den Abschnitt **Netzwerkmonitor**.

   Das folgende Fenster **Netzwerkmonitor** enthält auf der Registerkarte **Netzwerkaktivität** Informationen zur Netzwerkaktivität.

Auf einem Computer mit dem Betriebssystem Microsoft Windows Vista oder Microsoft Windows 7 kann der Netzwerkmonitor mit Hilfe des Kaspersky Gadgets geöffnet werden. Dafür muss eine der Schaltflächen des Kaspersky Gadgets mit der Funktion zum Öffnen des Fensters für den Netzwerkmonitor belegt sein (s. Abschnitt "Kaspersky Gadget verwenden" auf S. 63).

Um den Netzwerkmonitor mit Hilfe des Gadgets zu öffnen,

klicken Sie im Interface von Kaspersky Gadget auf die Schaltfläche mit dem Symbol **Netzwerkmonitor**.

Das folgende Fenster **Netzwerkmonitor** enthält auf der Registerkarte **Netzwerkaktivität** Informationen zur Netzwerkaktivität.

PROXYSERVER-EINSTELLUNGEN

Wenn die Internetverbindung über einen Proxyserver erfolgt, ist es erforderlich, die entsprechenden Verbindungseinstellungen anzupassen. Kaspersky Internet Security verwendet diese Einstellungen bei der Arbeit bestimmter Schutzkomponenten und für das Update der Datenbanken und Programm-Module.

Wenn in Ihrem Netzwerk ein Proxyserver installiert ist, der einen nicht standardmäßigen Port benutzt, ist es erforderlich, diesen Port zur Liste der kontrollierten Ports hinzuzufügen (s. Abschnitt "Liste der zu kontrollierenden Ports erstellen" auf S. 126).

Gehen Sie folgendermaßen vor, um die Verbindungseinstellungen für einen Proxyserver anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** die Komponente **Netzwerk**.

3. Klicken Sie im Block **Proxyserver** auf **Proxyserver-Einstellungen anpassen**.

4. Geben Sie im folgenden Fenster **Proxyserver-Einstellungen** die Verbindungseinstellungen für einen Proxyserver an.

LISTE DER ZU KONTROLLIERENDEN PORTS ERSTELLEN

Bei der Arbeit von Schutzkomponenten wie Mail-Anti-Virus, Anti-Spam, Web-Anti-Virus (auf S. 93) und IM-Anti-Virus werden die Datenströme kontrolliert, die mit bestimmten Protokollen und über bestimmte offene TCP-Ports Ihres Computers übertragen werden. Mail-Anti-Virus analysiert beispielsweise die Informationen, die per SMTP übertragen werden, während Web-Anti-Virus die HTTP-, HTTPS- und FTP-Pakete analysiert.

Sie können die Kontrolle aller oder nur bestimmter Netzwerkports aktivieren. Bei der Kontrolle bestimmter Ports kann eine Liste der Programme angelegt werden, für die alle Ports kontrolliert werden sollen. Es wird empfohlen, in diese Liste Programme aufzunehmen, die Daten per FTP-Protokoll senden oder empfangen.

➡ *Gehen Sie folgendermaßen vor, um einen Port zur Liste der kontrollierten Ports hinzuzufügen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Netzwerk**.
3. Wählen Sie im Block **Kontrollierte Ports** die Option **Nur ausgewählte Ports kontrollieren** aus und klicken Sie auf **Auswählen...**.

   Das Fenster **Netzwerkports** wird geöffnet.
4. Öffnen Sie über den Link **Hinzufügen**, unterhalb der Portliste im oberen Fensterbereich das Fenster **Netzwerkport** und geben Sie Nummer und Beschreibung des Ports ein.

➡ *Gehen Sie folgendermaßen vor, um einen Port aus der Liste der kontrollierten Ports auszuschließen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Netzwerk**.
3. Wählen Sie im Block **Kontrollierte Ports** die Option **Nur ausgewählte Ports kontrollieren** aus und klicken Sie auf **Auswählen...**.

   Das Fenster **Netzwerkports** wird geöffnet.
4. Deaktivieren Sie in der Portliste im oberen Fensterbereich das Kontrollkästchen neben der Beschreibung des Ports, der deaktiviert werden soll.

➡ *Gehen Sie folgendermaßen vor, um eine Liste der Programme anzulegen, für die alle Ports kontrolliert werden sollen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Netzwerk**.
3. Wählen Sie im Block **Kontrollierte Ports** die Option **Nur ausgewählte Ports kontrollieren** aus und klicken Sie auf **Auswählen...**.

   Das Fenster **Netzwerkports** wird geöffnet.
4. Aktivieren Sie das Kontrollkästchen **Alle Ports für die angegebenen Programme kontrollieren** und aktivieren Sie in der darunter angeordneten Programmliste die Kontrollkästchen neben den Programmen, für die alle Ports kontrolliert werden sollen.
5. Wenn ein erforderliches Programm nicht auf der Liste steht, können Sie es folgendermaßen hinzufügen:

   a. Klicken Sie auf den Link **Hinzufügen**, der sich unter der Programmliste befindet, um das Menü zu öffnen, und wählen Sie einen Punkt aus:

      - Um den Ort einer ausführbaren Programmdatei anzugeben, klicken Sie auf **Durchsuchen** und geben Sie den Ort der Datei auf dem Computer an.

- Klicken Sie auf **Programme**, um ein Programm aus der Liste der momentan aktiven Programme auszuwählen. Wählen Sie im folgenden Fenster **Programm auswählen** das erforderliche Programm.

b. Geben Sie im Fenster **Programm** eine Beschreibung für das gewählte Programm ein.

ANTI-SPAM

Anti-Spam erkennt unerwünschte E-Mails (Spam) und verarbeitet sie nach den Regeln Ihres Mailprogramms.

Anti-Spam wird als Erweiterungsmodul in folgende Mailprogramme integriert:

- Microsoft Office Outlook (auf S. 141).
- Microsoft Outlook Express (Windows Mail) (auf. S. 141).
- The Bat! (auf S. 142).
- Thunderbird (auf S. 142).

Mit Hilfe der Listen für verbotene und erlaubte Absender kann festgelegt werden, von welchen Adressen erwünschte E-Mails und von welchen Spam zu erwarten ist. Auch Nachrichten, die nicht an Sie adressiert sind (s. S. 136), lassen sich als Spam einordnen. Außerdem kann Anti-Spam eine E-Mail auf das Vorhandensein von erlaubten und verbotenen Phrasen sowie von Phrasen aus der Liste für anstößige Ausdrücke analysieren.

Eine Voraussetzung für die effektive Unterscheidung zwischen Spam und nützlichen E-Mails, ist ein Training von Anti-Spam (s. Abschnitt "Anti-Spam-Training" auf S. 129).

Anti-Spam verwendet einen lernfähigen Algorithmus, mit dem die Komponente mit der Zeit genauer zwischen Spam und erwünschter E-Mails unterscheiden kann. Als Datenquelle für den Algorithmus dient der Inhalt einer E-Mail.

Die Arbeit der Komponente Anti-Spam besteht aus zwei Etappen:

1. Anwendung von strengen Kriterien für die Filterung einer Nachricht. Diese Kriterien ermöglichen es, schnell festzustellen, ob eine Nachricht Spam ist. Anti-Spam weist der Nachricht den Status *Spam* oder *Kein Spam*, die Untersuchung wird beendet und die Nachricht zur Bearbeitung an das Mailprogramm weitergeleitet (siehe unten: Schritte 1–5).

2. Analyse von E-Mails, die bei der Filterung nicht eingestuft werden konnten. Solche Nachrichten lassen sich nicht eindeutig als Spam einordnen. Deshalb berechnet Anti-Spam die *Wahrscheinlichkeit*, mit der es sich bei einer Nachricht um Spam handelt.

Der Algorithmus für die Arbeit von Anti-Spam umfasst folgende Schritte:

1. Es wird geprüft, ob die Absenderadresse einer E-Mail auf den Listen für erlaubte und verbotene Absender steht.

   - Wenn die Absenderadresse auf der Liste der erlaubten Absender steht, erhält die Nachricht den Status *Kein Spam*.

   - Wenn die Absenderadresse auf der Liste der verbotenen Absender steht, erhält die Nachricht den Status *Spam*.

2. Wurde die Nachricht mit Hilfe von Microsoft Exchange Server gesendet und die Untersuchung solcher Nachrichten ist deaktiviert, dann erhält sie den Status *Kein Spam*.

3. Die Nachricht wird auf das Vorhandensein von Zeilen aus der Liste mit erlaubten Phrasen analysiert. Wenn mindestens eine Zeile aus dieser Liste gefunden wird, erhält die Nachricht den Status *Kein Spam*. Dieser Schritt wird standardmäßig übersprungen.

4. Es wird analysiert, ob die Nachricht Zeilen aus der Liste der verbotenen Phrasen und der Liste der anstößigen Phrasen enthält. Werden in einer Nachricht Wörter aus diesen Listen gefunden, so werden ihre gewichteten

Koeffizienten summiert. Wenn die Summe der Koeffizienten über 100 liegt, erhält die Nachricht den Status *Spam*. Dieser Schritt wird standardmäßig übersprungen.

5. Wenn der Nachrichtentext eine Adresse enthält, die in der Datenbank von verdächtigen oder Phishing-Adressen steht, erhält die Nachricht den Status *Spam*.
6. Die Nachricht wird mit Hilfe heuristischer Regeln analysiert. Wenn aufgrund dieser Analyse in E-Mails typische Spam-Merkmale gefunden werden, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt.
7. Die Nachricht wird mit Hilfe der GSG-Technologie analysiert. Dabei überprüft Anti-Spam die in der E-Mail enthaltenen Bilder. Wenn in den Bildern typische Spam-Merkmale gefunden werden, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt.
8. Dokumente des Formats RTF, die an eine E-Mail angehängt sind, werden analysiert. Anti-Spam sucht in angehängten Dokumenten nach typischen Spam-Merkmalen. Zum Abschluss der Analyse berechnet Anti-Spam, wie stark sich die Wahrscheinlichkeit erhöht hat, dass es sich bei der Nachricht um Spam handelt. Die Verwendung dieser Technologie ist standardmäßig deaktiviert.
9. Das Vorhandensein zusätzlicher Merkmale, die für Spam charakteristisch sind, wird überprüft. Jede Übereinstimmung erhöht die Wahrscheinlichkeit, dass es sich um Spam handelt.
10. Wenn mit Anti-Spam bereits ein Training ausgeführt wurde, wird die Nachricht mit Hilfe der iBayes-Technologie untersucht. Der lernfähige iBayes-Algorithmus berechnet die Wahrscheinlichkeit, mit der es sich bei der Nachricht um Spam handelt. Dazu wird analysiert, wie häufig im Text der Nachricht typische Spam-Phrasen vorkommen.

Ein Training wird nur dann ausgeführt, wenn in Kaspersky Internet Security die iBayes-Funktion für den lernfähigen Textanalyse-Algorithmus aktiviert ist. Diese Funktion ist nicht in allen Sprachversionen vorhanden.

Die Nachrichtenanalyse ergibt eine Wahrscheinlichkeit, mit der die E-Mail als Spam gilt. Diese Wahrscheinlichkeit wird durch den Wert des *Spam-Faktors* angegeben. Abhängig von den Grenzwerten für den Spam-Faktor wird einer Nachricht der Status *Spam* oder *potenzieller Spam* zugewiesen (s. Abschnitt "Grenzwerte für den Spam-Faktor regulieren" auf S. 138). Außerdem wird für Spam und potenziellen Spam im Feld **Betreff** standardmäßig die Markierung **[!! SPAM]** oder **[!! Probable Spam]** (s. Abschnitt "**Markierung zum Betreff einer Nachricht hinzufügen**" auf S. 139) hinzugefügt. Anschließend wird die Nachricht nach den von Ihnen definierten Regeln für Mailprogramme (s. Abschnitt "Spam-Verarbeitung in Mailprogrammen anpassen" auf S. 140) verarbeitet.

IN DIESEM ABSCHNITT

ANTI-SPAM AKTIVIEREN UND DEAKTIVIEREN

Anti-Spam ist standardmäßig aktiviert und arbeitet in dem Modus, der von Kaspersky Lab empfohlen wird. Bei Bedarf können Sie die Anti-Spam deaktivieren.

Gehen Sie folgendermaßen vor, um Anti-Spam zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Anti-Spam aktivieren**.

STUFE FÜR SPAM-SCHUTZ ÄNDERN UND WIEDERHERSTELLEN

Abhängig davon, wie häufig Sie Spam erhalten, können Sie eine der vordefinierten Spam-Schutzstufen auswählen oder Anti-Spam manuell anpassen. Die Stufen für den Spam-Schutz entsprechen den Sicherheitsstufen, die von den Kaspersky-Lab-Experten definiert wurden.

- **Hoch**. Diese Sicherheitsstufe sollte verwendet werden, wenn Sie sehr viel Spam erhalten, z.B. bei Verwendung eines kostenlosen Maildiensts. Bei Auswahl dieser Stufe kann die Häufigkeit steigen, dass erwünschte Post als Spam eingestuft wird.
- **Empfohlen**. Diese Sicherheitsstufe gilt für die meisten Situationen als empfohlen.
- **Niedrig**. Diese Sicherheitsstufe sollte verwendet werden, wenn Sie nur selten Spam erhalten, z.B. bei der Arbeit in einer geschützten Umgebung des internen Firmen-Mailsystems. Bei Auswahl dieser Stufe kann die Häufigkeit sinken, dass erwünschte Post als Spam oder potenzieller Spam eingestuft wird.

Während der Konfiguration von Anti-Spam können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese Einstellungen gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und entsprechen der Sicherheitsstufe **Empfohlen**.

Gehen Sie folgendermaßen vor, um die festgelegte Spam-Sicherheitsstufe zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

   Stellen Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** die erforderliche Sicherheitsstufe ein oder klicken Sie auf **Einstellungen**, um die Untersuchungseinstellungen manuell anzupassen.

   Wenn manuelle Änderungen erfolgen, ändert sich der Name der Sicherheitsstufe in **Benutzerdefiniert**.

Gehen Sie folgendermaßen vor, um die standardmäßigen Einstellungen für den Spam-Schutz wiederherzustellen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite im Block **Sicherheitsstufe** auf **Standard**.

ANTI-SPAM-TRAINING

Eines der Werkzeuge zur Spam-Erkennung ist der lernfähige iBayes-Algorithmus. Mit diesem Algorithmus wird auf Basis von Phrasen, die in einer Nachricht enthalten sind, darüber entschieden, welchen Status die Nachricht erhält. Bevor der iBayes-Algorithmus eingesetzt wird, benötigt Anti-Spam Zeilenmuster aus erwünschten Mails und aus Spam-Mails. Dazu dient ein *Training.*

Ein Training wird dann ausgeführt, wenn in Kaspersky Internet Security die iBayes-Funktion für den lernfähigen Textanalyse-Algorithmus aktiviert ist. Diese Funktion ist nicht in allen Sprachversionen vorhanden.

Es existieren mehrere Methoden für das Training von Anti-Spam:

- Anti-Spam-Training mit ausgehenden E-Mails.
- Training während der Arbeit mit E-Mails in einem Mailprogramm. Dazu dienen für das Training vorgesehene Schaltflächen und Menüpunkte.
- Training bei der Arbeit mit den Anti Spam-Berichten.

IN DIESEM ABSCHNITT

TRAINING MIT AUSGEHENDEN E-MAILS

Sie können Anti-Spam mit 50 ausgehenden E-Mails trainieren. Nachdem das Anti-Spam-Training aktiviert ist, wird jede von Ihnen gesendete Nachricht analysiert und als Muster für eine erwünschte Nachricht verwendet. Das Training wird abgeschlossen, nachdem 50 Nachrichten gesendet wurden.

➡ *Gehen Sie folgendermaßen vor, um das Anti-Spam-Training mit ausgehenden E-Mails zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Erweitert** im Block **Ausgehende E-Mails** das Kontrollkästchen **Mit ausgehenden E-Mails trainieren**.

Beim Training mit ausgehenden Nachrichten werden die entsprechenden Empfängeradressen automatisch zur Liste der erlaubten Absender hinzugefügt. Sie können diese Funktion deaktivieren (s. Abschnitt "Adressen zur Liste der erlaubten Absender hinzufügen" auf S. 131).

TRAINING ÜBER DIE OBERFLÄCHE EINES MAILPROGRAMMS

In der Symbolleiste und im Menü Ihres Mailprogramms stehen entsprechende Schaltflächen zur Verfügung, um Anti-Spam direkt bei der Arbeit mit E-Mails zu trainieren.

Die Schaltflächen und Menüpunkte für das Anti-Spam-Training erscheinen erst nach der Installation von Kaspersky Internet Security auf der Benutzeroberfläche der Mailprogramme.

➡ *Gehen Sie folgendermaßen vor, um Anti-Spam über die Oberfläche eines Mailprogramms zu trainieren:*

1. Starten Sie das Mailprogramm.

2. Wählen Sie eine Nachricht aus, mit deren Hilfe Sie Anti-Spam trainieren möchten.

3. Führen Sie - abhängig davon, welchen Mail-Client Sie verwenden - folgende Aktionen aus:

   - Klicken Sie in der Symbolleiste von Microsoft Office Outlook auf **Spam** oder **Kein Spam**.
   - Klicken Sie in der Symbolleiste von Microsoft Office Outlook (Windows Mail) auf **Spam** oder **Kein Spam**.
   - Verwenden Sie im Mailprogramm The Bat! die dafür vorgesehenen Punkte **Als Spam markieren** und **Als KEIN Spam markieren** im Menü **Extras**.
   - Verwenden Sie in der Symbolleiste von Mozilla Thunderbird die Schaltfläche **Spam/Kein Spam**.

Nachdem eine der oben genannten Aktionen ausgewählt wurde, führt Anti-Spam mit der ausgewählten Nachricht ein Training durch. Wenn Sie mehrere Nachrichten markieren, erfolgt das Training mit allen ausgewählten E-Mails.

Die Absenderadresse einer als erwünscht markierten Nachricht wird automatisch zur Liste der erlaubten Absender hinzugefügt. Sie können diese Funktion deaktivieren (s. Abschnitt "Adressen zur Liste der erlaubten Absender hinzufügen" auf S. 131).

ADRESSEN ZUR LISTE DER ERLAUBTEN ABSENDER HINZUFÜGEN

Beim Anti-Spam-Training im Fenster eines Mailprogramms werden erwünschte Absenderadressen automatisch zur Liste der erlaubten Absender hinzugefügt hinzugefügt (s. Abschnitt "Verbotene und erlaubte Absender" auf S. 135). Dieser Liste werden beim Training mit ausgehenden Nachrichten auch die Empfängeradressen der ausgehenden Mails hinzugefügt.

Sie können diese Funktion deaktivieren, damit die Trainingsergebnisse nicht automatisch zur Liste der erlaubten Absender hinzugefügt werden.

➡ *Gehen Sie folgendermaßen vor, damit Adressen nicht zur Liste für erlaubte Absender hinzugefügt werden:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie auf **Auswählen**.

   Das Fenster **Zulässige Absender** wird geöffnet.

5. Deaktivieren Sie das Kontrollkästchen **Bei Anti-Spam-Training Adressen von erlaubten Absendern hinzufügen**.

TRAINING MIT BERICHTEN

Es besteht die Möglichkeit, Anti-Spam auf Basis von Berichten zu trainieren. Solche Berichte enthalten Angaben über Nachrichten, die der Kategorie "potenzieller Spam" angehören. Beim Training erhalten Nachrichten die Markierung **Spam** oder **Kein Spam** und die Absender werden zur Liste für erlaubte oder verbotene Absender hinzugefügt (s. Abschnitt "Verbotene und erlaubte Absender" auf S. 135).

Nachrichten erhalten die Markierung **Spam** oder **Kein Spam**, wenn in Kaspersky Internet Security die iBayes-Funktion für den lernfähigen Textanalyse-Algorithmus aktiviert ist. Diese Funktion ist nicht in allen Sprachversionen vorhanden.

➡ *Gehen Sie folgendermaßen vor, um Anti-Spam an einem Bericht zu trainieren:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Bereich des Fensters auf **Berichte**.
3. Klicken Sie im folgenden Fenster **Berichte** auf die Schaltfläche **Detaillierter Bericht**.

   Das Fenster **Detaillierter Bericht** wird geöffnet.
4. Wählen Sie auf der linken Fensterseite den Abschnitt **Anti-Spam**.
5. Legen Sie im rechten Fensterbereich mit Hilfe der Einträge in der Spalte **Objekt** die Mails fest, mit denen Sie Anti-Spam trainieren möchten. Öffnen Sie für jede dieser Nachrichten durch Rechtsklick das Kontextmenü und wählen Sie eine entsprechende Aktion für die Nachricht:
   - Als Spam markieren.
   - Als Kein Spam markieren.
   - Zur Erlaubnisliste hinzufügen
   - Zur Verbotsliste hinzufügen

LINKS IN E-MAILS UNTERSUCHEN

Anti-Spam kann prüfen, ob die in E-Mails enthaltenen Links auf der Liste verdächtiger Webadressen oder auf der Liste für Phishing-Webadressen stehen. Diese Listen gehören zum Lieferumfang von Kaspersky Internet Security. Wenn Sie am Kaspersky Security Network teilnehmen (auf S. 184), wendet sich Kaspersky Internet Security auch zur Überprüfung von Links an das Kaspersky Security Network. Wenn ein Phishing-Link oder ein verdächtiger Link in einer Nachricht oder Phishing-Elemente im Nachrichtentext gefunden werden, wird die Nachricht als Spam eingestuft.

Für die Link-Untersuchung von E-Mails kann zusätzlich die heuristische Analyse verwendet werden.

➡ *Gehen Sie folgendermaßen vor, um die Link-Untersuchung mit den Datenbanken für verdächtige und Phishing-Adressen zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** die Kontrollkästchen **Mit Links aus der Datenbank für verdächtige Webadressen** und **Mit Phishing-Elementen**.

➡ *Gehen Sie folgendermaßen vor, um die Verwendung der heuristischen Analyse zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Klicken Sie auf der Registerkarte **Allgemein** unter **Folgende Nachrichten als Spam einstufen** auf **Erweitert**.

5. Aktivieren Sie im folgenden Fenster **Anti-Phishing anpassen** das Kontrollkästchen **Heuristische Analyse zur Phishing-Prüfung von E-Mails verwenden** und legen Sie mit dem Schieberegler eine Genauigkeitsstufe für die Untersuchung fest.

SPAM NACH PHRASEN UND ADRESSEN ERMITTELN. LISTEN ERSTELLEN

Sie können folgende Listen erstellen: Listen für erlaubte, verbotene und anstößige Schlüsselphrasen, Listen für erlaubte und verbotene Absenderadressen, Liste für Ihre eigenen Adressen. Beim Einsatz dieser Listen untersucht Anti-Spam den Nachrichteninhalt auf das Vorkommen von Wortverbindungen, die auf der Phrasenliste stehen, und die Absender- und Empfängeradressen auf Übereinstimmungen mit den Einträgen in den Adressenlisten. Wenn eine entsprechende Phrase oder Adresse gefunden wird, identifiziert Anti-Spam die Nachricht als erwünscht oder als Spam. Die Entscheidung ist davon abhängig, auf welcher Liste die gefundene Phrase oder Adresse steht.

Als Spam gelten Nachrichten:

- die verbotene oder anstößige Phrasen mit einem summierten gewichteten Koeffizienten von über 100 enthalten.
- die von einer verbotenen Adresse stammen oder nicht an Sie adressiert sind.

Als erwünscht gelten Nachrichten:

- die erlaubte Phrasen enthalten.
- die von einer erlaubten Adresse stammen.

IN DIESEM ABSCHNITT

PHRASEN- UND ADRESSENMASKEN VERWENDEN

In den Listen für erlaubte, verbotene und anstößige Phrasen können Masken für Phrasen verwendet werden. In den Listen für erlaubte und verbotene Absenderadressen sowie in der Liste der vertrauenswürdigen Adressen können Adressmasken verwendet werden.

Eine Maske ist eine bestimmte Zeile, mit der eine Phrase oder Adresse verglichen wird. Bestimmte Zeichen werden in einer Maske als Platzhalter für andere Zeichen eingesetzt: * steht für eine beliebige Zeichenfolge und ? für ein beliebiges Einzelzeichen. Wenn solche Zeichen in einer Maske verwendet werden, können mehrere Phrasen oder Adressen mit der Maske übereinstimmen (s. folgende Beispiele).

Wenn das Zeichen * oder ? in einer Phrase enthalten ist (z.B. Wie spät ist es?), muss ihm das Zeichen \ vorangestellt werden, damit es von Anti-Spam korrekt interpretiert wird. Anstelle des Zeichens * muss in der Maske also die Verbindung * verwendet werden und anstelle von ? die Verbindung \? (z.B. Wie spät ist es\?).

Beispiele für Phrasenmasken:

- Besuchen Sie unser*! – Dieser Maske entspricht eine Nachricht, die eine Phrase enthält, die mit den Wörtern "Besuchen Sie unser" beginnt, beliebig weitergeht und mit dem Zeichen ! endet.
- Angebot – Dieser Maske entspricht eine Nachricht, die eine Phrase enthält, die mit dem Wort "Angebot" beginnt, und beliebig weitergeht.

Beispiele für Adressmasken:

- admin@test.com – Dieser Maske entspricht nur die Adresse admin@test.com.
- admin@* – Dieser Maske entspricht die Adresse eines Absenders mit dem Namen admin, z.B. admin@test.com, admin@example.org.
- *@test* – Dieser Maske entspricht die Adresse eines beliebigen Absenders mit der Mail-Domain test, z.B. admin@test.com, info@test.org.
- info.*@test.??? – dieser Maske entspricht die Adresse eines beliebigen Absenders einer Nachricht, dessen Name mit info. beginnt und dessen Maildomäne mit test. anfängt, woraufhin drei beliebige Zeichen folgen, z.B.: info.product@test.com oder info.company@test.org, nicht jedoch info.product@test.ru.

VERBOTENE UND ERLAUBTE PHRASEN

In der Liste der *verbotenen Phrasen* können Sie Phrasen eintragen, die nach Ihrer Einschätzung für Spam charakteristisch sind, und für jede Phrase einen gewichteten Koeffizienten festlegen. Mit dem *gewichteten Koeffizienten* lässt sich angeben, wie charakteristisch eine Phrase für Spam-Nachrichten ist: Je höher der Koeffizient, desto wahrscheinlicher ist es, dass es sich bei einer Nachricht mit dieser Phrase um Spam handelt. Der gewichtete Koeffizient einer Phrase kann zwischen 0 und 100 liegen. Wenn die Summe der gewichteten Koeffizienten aller in einer Nachricht gefunden Phrasen über 100 liegt, wird die Nachricht als Spam betrachtet.

Schlüsselphrasen, die für erwünschte Nachrichten charakteristisch sind, können in die Liste für *erlaubte Phrasen* aufgenommen werden. Wenn eine solche Phrase in einer Nachricht gefunden wird, identifiziert Anti-Spam diese als erwünscht (Kein Spam).

In die Listen für verbotene und erlaubte Phrasen können vollständige Phrasen und entsprechende Masken eingetragen werden (s. Abschnitt "Phrasen- und Adressmasken verwenden" auf S. 133).

➡ *Gehen Sie folgendermaßen vor, um eine Liste mit verbotenen oder erlaubten Absendern zu erstellen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Gehen Sie auf der Registerkarte **Allgemein** folgendermaßen vor:
   - Wenn eine Liste für verbotene Phrasen erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Mit verbotenen Phrasen** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Verbotene Phrasen** wird geöffnet.
   - Wenn eine Liste für erlaubte Phrasen erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen **Mit erlaubten Phrasen** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Zulässige Phrasen** wird geöffnet.
5. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Verbotene Phrase** (oder das Fenster **Erlaubte Phrase**).

6. Geben Sie eine vollständige Phrase oder eine entsprechende Maske ein, legen Sie einen gewichteten Koeffizienten für die verbotene Phrase fest und klicken Sie anschließend auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster mit der Liste das entsprechende Kontrollkästchen zu deaktivieren.

ANSTÖßIGE PHRASEN

Im Lieferumfang von Kaspersky Internet Security befindet sich eine Liste mit anstößigen Phrasen, die Spezialisten von Kaspersky Lab erstellt haben. Die Liste enthält anstößige Phrasen, deren Vorhandensein in einer Nachricht mit großer Wahrscheinlichkeit darauf hinweist, dass es sich um Spam handelt. In diese Liste können vollständige Phrasen und entsprechende Masken eingetragen werden (s. Abschnitt "Phrasen- und Adressmasken verwenden" auf S. 133).

Wenn für einen Benutzer die Kindersicherung (s. S. 152) aktiviert ist und die Einstellungen der Kindersicherung durch ein Kennwort geschützt sind, ist das Kennwort (s. S. 67) erforderlich, um die Liste für anstößige Phrasen zu öffnen.

Gehen Sie folgendermaßen vor, um die Liste der anstößigen Phrasen zu ändern:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Mit verbotenen Phrasen** und klicken Sie auf **Auswählen**.

   Das Fenster **Verbotene Phrasen** wird geöffnet.

5. Aktivieren Sie das Kontrollkästchen **Anstößige Phrasen als verboten einstufen** und öffnen Sie mit dem Link **anstößige Phrasen** das Fenster **Vereinbarung**.

6. Lesen Sie den Vereinbarungstext. Wenn Sie den genannten Bedingungen zustimmen, aktivieren Sie unten das Kontrollkästchen und klicken Sie auf **OK**.

   Das Fenster **Anstößige Sprache** wird geöffnet.

7. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Verbotene Phrase**.

8. Geben Sie eine vollständige Phrase oder eine entsprechende Maske ein, legen Sie einen gewichteten Koeffizienten für die Phrase fest und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster mit der Liste das entsprechende Kontrollkästchen zu deaktivieren.

VERBOTENE UND ERLAUBTE ABSENDER

Zur Liste der *verbotenen Absender* können Sie Absenderadressen hinzufügen, deren Nachrichten von Anti-Spam als Spam identifiziert wurden. Absenderadressen, von denen kein Spam erwartet wird, stehen auf der Liste der *erlaubten Absender*. Diese Liste wird beim Training der Komponente Anti-Spam (s. Abschnitt "Adressen zur Liste der erlaubten Absender hinzufügen" auf S. 131) automatisch angelegt. Außerdem können Sie der Liste Einträge hinzufügen.

In die Listen für erlaubte und verbotene Absender können vollständige Adressen und Adressmasken eingetragen werden (s. Abschnitt "Phrasen- und Adressmasken verwenden" auf S. 133).

Gehen Sie folgendermaßen vor, um eine Liste mit erlaubten oder verbotenen Absendern zu erstellen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Gehen Sie auf der Registerkarte **Allgemein** folgendermaßen vor:

   - Wenn eine Liste für verbotene Absender erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als Spam einstufen** das Kontrollkästchen **Von verbotenen Absendern** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Verbotene Absender** wird geöffnet.

   - Wenn eine Liste für erlaubte Absender erstellt werden soll, aktivieren Sie im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie rechts auf **Auswählen**.

     Das Fenster **Zulässige Absender** wird geöffnet.

5. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Maske für E-Mail-Adresse**.

6. Geben Sie eine Adressmaske ein und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster mit der Liste das entsprechende Kontrollkästchen zu deaktivieren.

IHRE ADRESSEN

Sie können eine Liste mit Ihren E-Mail-Adressen anlegen, damit nicht an Sie adressierte Mails als Spam markiert werden

➡ *Gehen Sie folgendermaßen vor, um eine Liste mit Ihren Adressen anzulegen:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Nicht an mich adressiert** und klicken Sie auf **Meine Adressen**.

   Das Fenster **Meine Adressen** wird geöffnet.

5. Öffnen Sie mit dem Link **Hinzufügen** das Fenster **Maske für E-Mail-Adresse**.

6. Geben Sie eine Adressmaske ein und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, im Fenster mit der Liste das entsprechende Kontrollkästchen zu deaktivieren.

PHRASEN UND ADRESSEN EXPORTIEREN UND IMPORTIEREN

Listen mit Phrasen und Adressen können flexibel eingesetzt werden. Zum Beispiel können Adressen in eine entsprechende Liste auf einem anderen Computer übertragen werden, auf dem Kaspersky Internet Security installiert ist.

Dabei gilt folgendes Vorgehen:

1. *Exportieren* Sie eine Liste, d.h. die Einträge werden aus einer Liste in eine Datei kopiert.
2. Übertragen Sie die gespeicherte Datei auf einen anderen Computer (z.B. per E-Mail oder mit einem Wechseldatenträger).
3. *Importieren* Sie eine Liste, d.h. die Einträge werden aus einer Datei in eine entsprechende Liste auf einem anderen Computer eingetragen.

Beim Export einer Liste können Sie wählen, ob nur ausgewählte Listenelemente oder die gesamte Liste kopiert werden soll. Beim Import können der Liste neue Elemente hinzugefügt oder die vorhandene Liste durch eine importierte ersetzt werden.

Für Adressen aus der Liste erlaubter Absender ist der Import von Adressen oder eines Adressbuchs für Microsoft Office Outlook / Microsoft Outlook Express (Windows Mail) möglich.

➡ *Gehen Sie folgendermaßen vor, um die Einträge aus einer Liste zu exportieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen in der Zeile mit dem Namen der Liste, aus der die Einträge exportiert werden sollen. Klicken Sie dann rechts auf die entsprechende Schaltfläche.
5. Aktivieren Sie im folgenden Fenster in der Liste die Kontrollkästchen für die Einträge, die in die Datei aufgenommen werden sollen.
6. Klicken Sie auf den Link **Export**.

   Im folgenden Fenster können Sie wählen, welche Elemente exportiert werden sollen. Führen Sie hier eine der folgenden Aktionen aus:

   - Klicken Sie auf **Ja**, wenn nur ausgewählte Einträge in die Datei aufgenommen werden sollen.
   - Klicken Sie auf **Nein**, wenn die gesamte Liste aufgenommen werden soll.
7. Geben Sie im folgenden Fenster einen Typ und einen Namen für die zu speichernde Datei an und bestätigen Sie das Speichern.

➡ *Gehen Sie folgendermaßen vor, um die Einträge aus einer Datei in eine Liste zu importieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen in der Zeile mit dem Namen der Liste, in den die Einträge importiert werden sollen. Klicken Sie dann rechts auf die entsprechende Schaltfläche.
5. Klicken Sie im Fenster auf den Link **Import**. Wenn Sie eine Liste mit erlaubten Absendern importieren, wählen Sie im folgenden Menü den Punkt **Aus Datei importieren**. Für die übrigen Listen muss kein Menüpunkt gewählt werden.

Wenn die Liste nicht leer ist, wird Ihnen im folgenden Fenster vorgeschlagen, die zu importierenden Elemente hinzuzufügen. Führen Sie hier eine der folgenden Aktionen aus:

- Klicken Sie auf **Ja**, wenn die Dateieinträge zur Liste hinzugefügt werden sollen.
- Klicken Sie auf **Nein**, wenn die vorhandenen Einträge durch die Liste aus der Datei ersetzt werden sollen.

6. Wählen Sie im folgenden Fenster eine Datei mit den zu importierenden Einträgen.

➧ *Gehen Sie folgendermaßen vor, um eine Liste mit erlaubten Absendern aus einem Adressbuch zu importieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Allgemein** im Block **Folgende Nachrichten als nützlich einstufen** das Kontrollkästchen **Von erlaubten Absendern** und klicken Sie auf **Auswählen**.

   Das Fenster **Zulässige Absender** wird geöffnet.
5. Klicken Sie auf den Link **Import**, öffnen Sie das Menü zur Auswahl einer Quelle und wählen Sie den Punkt **Aus Adressbuch importieren**.
6. Wählen Sie im folgenden Fenster das entsprechende Adressbuch.

GRENZWERTE FÜR DEN SPAM-FAKTOR REGULIEREN

Die Spam-Erkennung basiert auf der Verwendung moderner Filtertechnologien, die es erlauben, Anti-Spam so zu trainieren (s. Abschnitt "Anti-Spam-Training" auf S. 129), dass er relativ genau zwischen Spam, potenziellem Spam und erwünschten Mails unterscheiden kann. Dabei erhält jedes Element einer erwünschten oder einer Spam-Mail einen Koeffizienten.

Wenn eine E-Mail in Ihrer Mailbox eintrifft, untersucht Anti-Spam die Nachricht auf das Vorhandensein von Elementen, die für Spam und erwünschte Post charakteristisch sind. Die Koeffizienten für jedes Element einer erwünschten oder einer Spam-Mail werden summiert, und ein *Spam-Faktor* wird errechnet. Je höher der Spam-Faktor, desto höher ist die Wahrscheinlichkeit, mit der es sich bei einer Nachricht um Spam handelt. In der Grundeinstellung gilt eine Nachricht mit einem Spam-Faktor bis 60 als erwünscht. Bei einem Spam-Faktor von über 60 gilt eine Nachricht als potenzieller Spam. Wenn der Wert über 90 liegt, wird eine Nachricht als Spam betrachtet. Sie können die Grenzwerte für den Spam-Faktor ändern.

➧ *Gehen Sie folgendermaßen vor, um die Grenzwerte für den Spam-Faktor zu ändern:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Passen Sie auf der Registerkarte **Algorithmus** im Block **Spam-Faktor** den Wert des Spam-Faktors an. Dazu dient der Schieberegler oder das Eingabefeld mit Pfeiltasten.

ZUSÄTZLICHE MERKMALE, DIE DEN SPAM-FAKTOR BEEINFLUSSEN, VERWENDEN

Das Ergebnis für den Spam-Faktor kann durch zusätzliche Nachrichtenmerkmale beeinflusst werden: beispielsweise das Fehlen einer Empfängeradresse im Feld "An" oder eine zu lange Betreffzeile (über 250 Zeichen). Wenn eine Nachricht diese Merkmale aufweist, erhöht sich die Wahrscheinlichkeit, dass es sich um Spam handelt. Der Wert für den Spam-Faktor erhöht sich entsprechend. Sie können wählen, welche Zusatzmerkmale bei der Nachrichtenanalyse berücksichtigt werden sollen.

Gehen Sie folgendermaßen vor, um Zusatzmerkmale zu verwenden, die den Spam-Faktor erhöhen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Klicken Sie auf der Registerkarte **Algorithmus** auf **Erweitert**.
5. Aktivieren Sie im folgenden Fenster **Erweitert** die Kontrollkästchen für die Merkmale, die bei der Nachrichtenanalyse berücksichtigt werden sollen, um den Spam-Faktor zu erhöhen.

ALGORITHMUS ZUR SPAM-ERKENNUNG WÄHLEN

Anti-Spam analysiert E-Mail-Nachrichten unter Verwendung eines Algorithmus zur Spam-Erkennung.

Gehen Sie folgendermaßen vor, um die Verwendung eines Spam-Erkennungsalgorithmus für die E-Mail-Analyse zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.
3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.
4. Aktivieren Sie auf der Registerkarte **Algorithmus** im Block **Erkennungsalgorithmen** die entsprechenden Kontrollkästchen.

MARKIERUNG ZUM BETREFF EINER NACHRICHT HINZUFÜGEN

Anti-Spam kann Nachrichten, die sich bei der Untersuchung als Spam oder potenzieller Spam erweisen, im Feld **Betreff** spezielle Markierungen hinzufügen:

- **[!! SPAM]** – für Nachrichten, die als Spam identifiziert wurden.
- **[?? Probable Spam]** – für Nachrichten, die als potenzieller Spam identifiziert wurden.

Solche Markierungen in der Betreffzeile können Ihnen bei der Durchsicht von Nachrichtenlisten behilflich sein, Spam und potenziellen Spam aufzufinden.

Gehen Sie folgendermaßen vor, um die Option anzupassen, mit der dem Nachrichtenbetreff eine Markierung hinzugefügt wird:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Aktivieren Sie auf der Registerkarte **Erweitert** im Block **Aktionen** die Kontrollkästchen für die Markierungen, die dem Betreff hinzugefügt werden sollen. Ändern Sie bei Bedarf den Hinweistext.

NACHRICHTEN FÜR MICROSOFT EXCHANGE SERVER UNTERSUCHEN

In der Grundeinstellung werden Nachrichten für Microsoft Exchange Server nicht von Anti-Spam untersucht. Sie können die Untersuchung von E-Mails aktivieren, die im Rahmen eines internen Netzwerks verschickt werden (z.B. Firmenpost).

E-Mails werden als interne Mail betrachtet, wenn auf allen Netzwerkcomputern als Mail-Client das Programm Microsoft Office Outlook benutzt wird und die Benutzermailboxen sich auf einem Exchange-Server oder auf verbundenen Servern befinden.

➧ *Gehen Sie folgendermaßen vor, um die Untersuchung von Nachrichten für Microsoft Exchange Server zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Spam**.

3. Klicken Sie auf der rechten Fensterseite auf **Einstellungen**.

   Das Fenster **Anti-Spam** wird geöffnet.

4. Deaktivieren Sie auf der Registerkarte **Erweitert** im Block **Ausnahmen** das Kontrollkästchen **E-Mails für Microsoft Exchange Server nicht untersuchen**.

SPAM-VERARBEITUNG IN MAILPROGRAMMEN ANPASSEN

Wenn sich aufgrund einer Untersuchung ergibt, dass eine Nachricht als Spam oder potenzieller Spam gilt, sind die weiteren Aktionen von Anti-Spam vom Status der Nachricht und von der gewählten Aktion abhängig. Standardmäßig werden E-Mails, die als Spam oder potenzieller Spam gelten, modifiziert: Einer Nachricht wird im Feld **Betreff** die Markierung **[!! SPAM]** oder **[?? Probable Spam]** hinzugefügt (s. Abschnitt "Markierung zum Betreff einer Nachricht hinzufügen" auf S. 139).

Sie können Zusatzaktionen für Spam und potenziellen Spam festlegen. In den Mailprogrammen Microsoft Office Outlook und Microsoft Outlook Express (Windows Mail) sind dafür spezielle Erweiterungsmodule vorgesehen. Für die Mailprogramme The Bat! und Thunderbird können Sie Regeln für die E-Mail-Filterung erstellen.

IN DIESEM ABSCHNITT

MICROSOFT OFFICE OUTLOOK

E-Mails, die Anti-Spam als Spam oder potenziellen Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet. Wenn es erforderlich ist, Nachrichten nach der Untersuchung durch Anti-Spam zusätzlich zu verarbeiten, können Sie Microsoft Office Outlook entsprechend anpassen. Das Einstellungsfenster für die Spam-Bearbeitung erscheint automatisch, wenn das Mailprogramm nach der Installation von Kaspersky Internet Security zum ersten Mal gestartet wird. Die Einstellungen für die Verarbeitung von Spam und potenziellen Spam stehen außerdem in Microsoft Office Outlook auf der speziellen Registerkarte **Anti-Spam** im Menü **Extras** → **Optionen** zur Verfügung.

MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

E-Mails, die Anti-Spam als Spam oder potenziellen Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet. Wenn es erforderlich ist, Nachrichten nach der Untersuchung durch Anti-Spam zusätzlich zu verarbeiten, können Sie Microsoft Office Outlook (Windows Mail) entsprechend anpassen.

Das Einstellungsfenster für die Spam-Verarbeitung erscheint, wenn das Mailprogramm nach der Installation der Anwendung zum ersten Mal gestartet wird. Es kann auch mit der Schaltfläche **Einstellungen** geöffnet werden, die sich neben den Schaltflächen **Spam** und **Kein Spam** auf der Symbolleiste befindet.

REGEL FÜR DIE SPAM-UNTERSUCHUNG VON NACHRICHTEN ERSTELLEN

Im Folgenden wird erklärt, wie Spam-Regeln für die Nachrichtenverarbeitung mit Anti-Spam im Mailprogramm Microsoft Office Outlook erstellt werden. Auf Basis dieser Anleitung können Sie eine eigene Regel erstellen.

➧ *Gehen Sie folgendermaßen vor, um eine Regel zur Spam-Verarbeitung von Nachrichten zu erstellen:*

1. Starten Sie das Programm Microsoft Office Outlook und verwenden Sie den Befehl **Extras →Regeln und Benachrichtigungen** im Programmhauptfenster. Die Methode für den Start des Assistenten ist von der Microsoft Office Outlook-Version abhängig, die Sie verwenden. In dieser Hilfe wird das Erstellen einer Regel mit Hilfe von Microsoft Office Outlook 2003 beschrieben.

2. Gehen Sie im Fenster **Regeln und Benachrichtigungen** auf die Registerkarte **Regeln für E-Mails** und klicken Sie auf **Neu**. Dadurch wird der Assistent zum Erstellen einer neuen Regel gestartet. Er besteht aus einer Folge von Fenstern / Schritten:

   a. Sie können wählen, ob zum Erstellen der Regel eine Vorlage benutzt werden soll oder nicht. Wählen Sie die Variante **Regel ohne Vorlage erstellen** und wählen Sie als Prüfungsbedingung **Nachrichten bei Ankunft prüfen**. Klicken Sie auf **Weiter**.

   b. Klicken Sie im Fenster zur Auswahl der Bedingungen für die Nachrichtenprüfung auf **Weiter**, ohne ein Kontrollkästchen zu aktivieren. Bestätigen Sie in der Bestätigungsanfrage die Anwendung dieser Regel auf alle Nachrichten, die Sie erhalten.

   c. Aktivieren Sie im Fenster zur Auswahl der Aktionen für die Nachrichten in der Aktionsliste das Kontrollkästchen **diese mit einer vordefinierten Aktion bearbeiten**. Klicken Sie im unteren Bereich des Fensters auf den Link **einer vordefinierten Aktion**. Wählen Sie aus der Dropdown-Liste den Wert **Kaspersky Anti-Spam** und klicken Sie auf **OK**.

   d. Klicken Sie im Fenster zur Auswahl von Ausnahmen auf **Weiter**, ohne ein Kontrollkästchen zu aktivieren.

   e. Im Fenster zum Abschluss der Regelerstellung können Sie den Namen der Regel ändern (standardmäßig lautet er Kaspersky Anti-Spam). Überprüfen Sie, ob das Kontrollkästchen **Diese Regel aktivieren** aktiviert ist und klicken Sie auf **Fertig**.

3. Die neue Regel wird standardmäßig an erste Stelle zur Regelliste im Fenster **Regeln und Benachrichtigungen** hinzugefügt. Wenn Sie möchten, dass die Regel zuletzt auf eine Nachricht angewandt wird, verschieben Sie sie an das Ende der Liste.

Alle Nachrichten, die in der Mailbox ankommen, werden auf der Grundlage von Regeln bearbeitet. Die Verwendungsreihenfolge der Regeln hängt von der Priorität ab, die den einzelnen Regeln zugewiesen wurde. Die Regeln werden der Reihe nach angewendet. Die oberste Regel besitzt die höchste Priorität. Sie können die Anwendungspriorität der Regeln für Nachrichten erhöhen oder senken. Dazu wird eine Regel in der Liste nach oben oder unten verschoben. Wenn Sie nicht möchten, dass eine Nachricht zusätzlich nach einer Anti-Spam-Regel bearbeitet wird, nachdem bereits eine Regel angewandt wurde, muss in den Parametern dieser Regel das Kontrollkästchen **keine weiteren Regeln anwenden** aktiviert werden (s. Schritt 3. zum Erstellen der Regel).

THE BAT!

Die Aktionen für Spam und potenziellen Spam werden im Mailprogramm The Bat! mit den Mitteln des Mailprogramms festgelegt.

➡ *Gehen Sie folgendermaßen vor, um in The Bat! die Spam-Verarbeitungsregeln anzupassen:*

1. Wählen Sie im Menü **Optionen** des Mailprogramms den Punkt **Benutzereinstellungen**.

2. Wählen Sie in der Konfigurationsstruktur das Objekt **Spam-Schutz**.

Die angezeigten Einstellungen für den Spam-Schutz gelten für alle auf dem Computer installierten Anti-Spam-Module, die die Arbeit mit The Bat! unterstützen.

Sie müssen eine Score-Stufe festlegen und die Aktion angeben, die auf Nachrichten angewandt werden soll, denen ein bestimmter Score zugewiesen wurde (im Fall von Anti-Spam ist das die Wahrscheinlichkeit, dass eine E-Mail als Spam gilt):

- Nachricht mit einem Score, der den Grenzwert überschreitet, löschen.
- Nachricht mit einem bestimmten Score in einen speziellen Ordner für Spam-Nachrichten verschieben.
- Spam-Nachrichten, die mit einer speziellen Kopfzeile markiert sind, in den Spam-Ordner verschieben.
- Spam-Nachrichten im Ordner **Eingang** belassen.

Aufgrund der Bearbeitung von E-Mail-Nachrichten durch Kaspersky Internet Security wird der Nachricht auf der Basis eines Faktors, den Sie festlegen können, der Status Spam oder potenzieller Spam zugewiesen. Im Mailprogramm The Bat! ist ein entsprechender Score-Algorithmus für Nachrichten realisiert, der den Gegenstand Spam betrifft, und ebenfalls auf dem Spam-Faktor basiert. Um Differenzen zwischen den Spam-Faktoren in Kaspersky Internet Security und in The Bat! zu vermeiden, werden alle von Anti-Spam geprüften Nachrichten dem Rating angepasst, das dem Status der Nachricht entspricht: erwünschte E-Mails – 0%, potenzieller Spam – 50%, Spam – 100%. Dadurch stimmt der Score der Nachricht im Mailprogramm The Bat! nicht mit dem in Anti-Spam festgelegten Spam-Faktor überein, sondern mit dem Faktor des entsprechenden Status.

Einzelheiten über den Spam-Score und die Verarbeitungsregeln s. Dokumentation zum Mailprogramm The Bat!.

THUNDERBIRD

E-Mails, die Anti-Spam als Spam oder potenziellen Spam klassifiziert, werden im Feld **Betreff** standardmäßig durch die Markierungen **[!! SPAM]** oder **[?? Probable Spam]** gekennzeichnet. Wenn es nach einer Untersuchung durch Anti-Spam erforderlich ist, die Nachrichten zusätzlich zu verarbeiten, können Sie Thunderbird entsprechend anpassen. Öffnen Sie dazu mit dem Menübefehl **Extras** → **Filter** das Konfigurationsfenster (Details über die Arbeit mit dem Mail-Client s. Hilfe zu Mozilla Thunderbird).

Das Anti-Spam-Erweiterungsmodul für Thunderbird erlaubt es, ein Training mit E-Mails vorzunehmen, die mit diesem Mail-Client empfangen und gesendet wurden. Außerdem kann die E-Mail-Korrespondenz auf Spam untersucht werden. Das Modul wird in Thunderbird integriert und leitet E-Mails zur Untersuchung an die Komponente Anti-Spam um. Dazu dient der Menübefehl **Extras** → **Junk-Filter auf Ordner anwenden**. Die Nachrichtenuntersuchung wird also nicht von Thunderbird, sondern von Kaspersky Internet Security ausgeführt. Dabei bleibt die Funktionalität von Thunderbird unverändert.

Der Status des Anti-Spam-Erweiterungsmoduls wird in Form eines Symbols in der Statuszeile von Thunderbird angezeigt. Das graue Symbol bedeutet, dass bei der Arbeit des Plug-ins ein Problem vorliegt oder dass die Komponente Anti-Spam deaktiviert wurde. Das Konfigurationsfenster von Kaspersky Internet Security kann durch Doppelklick auf das Symbol geöffnet werden. Um zu den Einstellungen für Anti-Spam zu gelangen, klicken Sie im Block **Anti-Spam** auf **Einstellungen.**

ANTI-BANNER

Anti-Banner dient dazu, die Anzeige von Bannern auf den von Ihnen besuchten Webseiten und im Interface bestimmter Computerprogramme zu blockieren. Bannerwerbung kann Sie von der Arbeit ablenken und der Download von Bannern verursacht erhöhten Datenverkehr.

Bevor ein Banner auf einer Webseite oder im Fenster eines Computerprogramms angezeigt wird, muss es aus dem Internet geladen werden. Anti-Banner prüft die Adresse, von der ein Banner geladen wird. Stimmt die Adresse mit einer Maske aus der im Lieferumfang von Kaspersky Internet Security enthaltenen Liste oder der von Ihnen angelegten Schwarzen Bannerliste überein, wird das Banner blockiert. Zum Sperren von Bannern, deren Adressmasken nicht in den genannten Listen enthalten sind, wird eine heuristische Analyse verwendet.

Zusätzlich kann eine Weiße Liste mit erlaubten Adressen angelegt werden, auf deren Basis die Banneranzeige erlaubt wird.

IN DIESEM ABSCHNITT

ANTI-BANNER AKTIVIEREN UND DEAKTIVIEREN

Anti-Banner ist nach der Installation von Kaspersky Internet Security deaktiviert und blockiert die Banneranzeige nicht. Anti-Banner muss aktiviert werden, damit Banner blockiert werden.

Wenn alle Banner angezeigt werden sollen, muss Anti-Banner ausgeschaltet werden. Für bestimmte Banner kann es erforderlich sein, sie zur Liste für erlaubte Banner-Adressen hinzuzufügen (s. Abschnitt "Listen für verbotene und erlaubte Banner-Adressen erstellen" auf S. 144), damit sie angezeigt werden.

➡ *Gehen Sie folgendermaßen vor, um Anti-Banner zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
3. Aktivieren Sie im rechten Fensterbereich das Kontrollkästchen **Anti-Banner aktivieren**.

UNTERSUCHUNGSMETHODEN WÄHLEN

Sie können die Methoden festlegen, mit denen Anti-Banner Adressen untersuchen soll, von denen Banner geladen werden können: Zusätzlich zu diesen Methoden untersucht Anti-Banner die Banner-Adressen auf Übereinstimmung mit Masken aus den Listen für erlaubte und verbotene Adressen, falls diese Listen verwendet werden.

➡ *Gehen Sie folgendermaßen vor, um festzulegen, mit welchen Methoden Anti-Banner Adressen untersuchen soll:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.

3. Aktivieren Sie auf der rechten Fensterseite in der Gruppe **Untersuchungsmethoden** die Kontrollkästchen der zu verwendenden Methoden.

LISTEN FÜR VERBOTENE UND ERLAUBTE BANNER-ADRESSEN ERSTELLEN

Mit Hilfe von Listen für verbotene und erlaubte Banner-Adressen lässt sich festlegen, von welchen Adressen der Download und die Anzeige von Bannern verboten bzw. erlaubt werden sollen. Anti-Banner blockiert den Download und die Anzeige der Banner von Adressen, die den Masken entsprechen, die auf der von Ihnen angelegten Schwarzen Liste stehen. Anti-Banner erlaubt den Download und die Anzeige der Banner von Adressen, die den Masken entsprechen, die auf der von Ihnen angelegten Weißen Liste stehen.

Bei Verwendung der Browser Microsoft Internet Explorer, Mozilla Firefox und Google Chrome können der Liste für verbotene Adressen direkt aus dem Browserfenster Masken hinzugefügt werden.

➧ *Gehen Sie folgendermaßen vor, um eine Maske zur Liste der verbotenen oder erlaubten Adressen hinzuzufügen:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.

3. Aktivieren Sie auf der rechten Fensterseite im Block **Erweitert** das Kontrollkästchen **Liste der verbotenen Webadressen verwenden** (oder **Liste der erlaubten Webadressen verwenden**) und klicken Sie unter dem Kontrollkästchen auf **Einstellungen**.

   Das Fenster **Verbotene Adressen** (oder **Erlaubte Adressen**) wird geöffnet.

4. Klicken Sie auf **Hinzufügen**.

   Das Fenster **Adressmaske (URL**) wird geöffnet.

5. Geben Sie eine Banner-Maske an und klicken Sie auf **OK**.

Damit eine bestimmte Maske nicht mehr verwendet wird, muss sie nicht gelöscht werden. Es ist ausreichend, in der Liste das entsprechende Kontrollkästchen zu deaktivieren.

➧ *Um vom Browserfenster aus eine Maske zur Liste der verbotenen Adressen hinzuzufügen,*

öffnen Sie im Browserfenster durch Rechtsklick auf das Symbol das Kontextmenü und wählen Sie den Punkt **Zu Anti-Banner hinzufügen**.

ADRESSENLISTEN EXPORTIEREN / IMPORTIEREN

Die Listen für erlaubte und verbotene Banner-Adressen können mehrfach eingesetzt werden (Die Banner-Adressen können beispielsweise in eine entsprechende Liste auf einem anderen Computer übertragen werden, auf dem Kaspersky Internet Security installiert ist).

Dabei gilt folgendes Vorgehen:

1. *Exportieren* Sie eine Liste, d.h. die Einträge werden aus einer Liste in eine Datei kopiert.

2. Übertragen Sie die gespeicherte Datei auf einen anderen Computer (z.B. per E-Mail oder mit einem Wechseldatenträger).

3. *Importieren* Sie eine Liste, d.h. die Einträge werden aus einer Datei in eine entsprechende Liste auf einem anderen Computer eingetragen.

Beim Export einer Liste können Sie wählen, ob nur ausgewählte Listenelemente oder die gesamte Liste kopiert werden soll. Beim Import können der Liste neue Elemente hinzugefügt oder die vorhandene Liste durch eine importierte ersetzt werden.

Gehen Sie folgendermaßen vor, um Banner-Adressen aus der Liste für erlaubte oder verbotene Banner-Adressen zu exportieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
3. Klicken Sie auf der rechten Fensterseite im Block **Erweitert** in der Zeile mit dem Namen der Liste, aus der Adressen in eine Datei kopiert werden sollen, auf **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Erlaubte Adressen** (oder im Fenster **Verbotene Adressen**) die Kontrollkästchen der Adressen, die in die Datei aufgenommen werden sollen.
5. Klicken Sie auf **Export**.

   Im folgenden Fenster können Sie wählen, welche Elemente exportiert werden sollen. Führen Sie hier eine der folgenden Aktionen aus:

   - Klicken Sie auf **Ja**, wenn nur ausgewählte Adressen in die Datei aufgenommen werden sollen.
   - Klicken Sie auf **Nein**, wenn die gesamte Liste in die Datei aufgenommen werden soll.
6. Geben Sie im folgenden Fenster einen Namen für die zu speichernde Datei ein und bestätigen Sie das Speichern.

Gehen Sie folgendermaßen vor, um Banner-Adressen aus einer Datei in eine Liste für erlaubte oder verbotene Adressen zu importieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Schutz-Center** die Komponente **Anti-Banner**.
3. Klicken Sie auf der rechten Fensterseite im Block **Erweitert** in der Zeile mit dem Namen der Liste, zu der Adressen aus einer Datei hinzugefügt werden sollen, auf **Einstellungen**.
4. Klicken Sie im folgenden Fenster **Erlaubte Adressen** (oder im Fenster **Verbotene Adressen**) auf **Import**.

   Wenn die Liste nicht leer ist, wird Ihnen im folgenden Fenster vorgeschlagen, die zu importierenden Elemente hinzuzufügen. Führen Sie hier eine der folgenden Aktionen aus:

   - Klicken Sie auf **Ja**, wenn die Dateieinträge zur Liste hinzugefügt werden sollen.
   - Klicken Sie auf **Nein**, wenn die vorhandenen Einträge durch die Liste aus der Datei ersetzt werden sollen.
5. Wählen Sie im folgenden Fenster eine Datei mit den zu importierenden Einträgen.

SICHERE UMGEBUNG UND SICHERER BROWSER

Kaspersky Internet Security ermöglicht es, potenziell gefährliche Aktionen vom primären Betriebssystem isoliert auszuführen. Dafür sind in Kaspersky Internet Security folgende Optionen vorgesehen:

- ein bestimmtes Programm im sicheren Modus auf dem normalen Desktop starten (s. S. 55).
- in der Sicheren Umgebung arbeiten (s. S. 146).
- im Sicheren Browser arbeiten (s. S. 149).

Eine Isolierung vom primären Betriebssystem bietet Ihrem Computer zusätzliche Sicherheit, da reale Objekte des Betriebssystems nicht verändert werden.

Verdächtige Dateien, die bei der Arbeit im isolierten Modus gefunden werden, werden im normalen Modus in die Quarantäne verschoben. Wenn Dateien aus der Quarantäne wiederhergestellt werden, erfolgt die Wiederherstellung im ursprünglichen Ordner. Wenn ein Ursprungsordner nicht gefunden werden kann, bietet Kaspersky Internet Security an, einen Wiederherstellungsort für das Objekt anzugeben, der sich in jener Umgebung befindet (primäre oder sichere Umgebung), in der der Wiederherstellungsvorgang gestartet wurde.

Auf Computern mit Microsoft Windows XP x64 sind die Sichere Umgebung und der sichere Browser nicht verfügbar.

Auf Computern, die von Microsoft Windows XP x64 und Microsoft Windows 7 x64 verwaltet werden, kann die Funktionalität bestimmter Programme bei der Arbeit in der Sicheren Umgebung eingeschränkt sein. Beim Start solcher Programme erscheint eine entsprechende Meldung auf dem Bildschirm, wenn die Meldungen über das Ereignis (s. S. 182) **Die Funktionalität des Programms in der Sicheren Umgebung ist eingeschränkt** aktiviert wurden. Außerdem steht der sichere Desktop für den Start von Programmen nicht zur Verfügung.

IN DIESEM ABSCHNITT

ÜBER DIE SICHERE UMGEBUNG

Die Sichere Umgebung ist vom primären Betriebssystem isoliert. Sie dient zum Start von Programmen, an deren Sicherheit Zweifel bestehen. Bei der Arbeit in der Sicheren Umgebung werden Objekte, die tatsächlich zum Betriebssystem gehören, nicht verändert. Selbst wenn Sie in der Sicheren Umgebung ein infiziertes Programm starten, bleiben seine Aktionen auf die virtuelle Umgebung beschränkt und haben keinen Einfluss auf das Betriebssystem.

IN DIESEM ABSCHNITT

ARBEIT IN DER SICHEREN UMGEBUNG STARTEN UND BEENDEN

Die Sichere Umgebung kann auf folgende Arten gestartet werden:

- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 35).
- aus dem Kontextmenü von Kaspersky Internet Security (s. Abschnitt "Kontextmenü" auf S. 34).
- mit Hilfe der entsprechenden Schaltfläche im Interface von Kaspersky Gadget, wenn für diese die Funktion zum Start des sicheren Desktops festgelegt ist (s. Abschnitt "Kaspersky Gadget verwenden" auf S. 63).

- mit Hilfe einer Verknüpfung auf dem Desktop (s. Abschnitt "Auf dem Desktop eine Verknüpfung für die Sichere Umgebung erstellen" auf S. 149).

Die Sichere Umgebung kann auf folgende Weise beendet werden:

- über das **Startmenü** des Betriebssystems
- aus der Popup-Symbolleiste (s. Abschnitt "Popup-Symbolleiste in der Sicheren Umgebung verwenden" auf S. 148)
- mit der Tastenkombination **STRG+ALT+UMSCHALT+K**

➡ *Gehen Sie folgendermaßen vor, um die Sichere Umgebung aus dem Hauptfenster von Kaspersky Internet Security zu starten:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Sichere Umgebung** aus.
3. Klicken Sie im folgenden Fenster auf **Weiter zur Sicheren Umgebung**.

➡ *Um die Sichere Umgebung aus dem Kontextmenü von Kaspersky Internet Security zu starten,*

klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol von Kaspersky Internet Security, um das Kontextmenü zu öffnen, und wählen Sie dort den Punkt **Sichere Umgebung**.

➡ *Um die Sichere Umgebung aus dem Kaspersky Gadget zu starten,*

klicken Sie im Interface von Kaspersky Gadget auf die Schaltfläche mit dem Symbol **Sichere Umgebung** (nur für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7).

➡ *Um die Arbeit in der Sicheren Umgebung über das Startmenü zu beenden,*

wählen Sie im **Startmenü** des Betriebssystems den Punkt **Sichere Umgebung – Beenden**.

➡ *Gehen Sie folgendermaßen vor, um die Arbeit in der Sicheren Umgebung aus der Popup-Symbolleiste zu beenden,*

1. Zeigen Sie mit der Maus auf den oberen Bildschirmbereich.
2. Klicken Sie in der Popup-Symbolleiste auf die Schaltfläche .
3. Wählen Sie im folgenden Fenster zur Auswahl der Aktion den Punkt **Deaktivieren**.

PROGRAMME AUTOMATISCH IN DER SICHEREN UMGEBUNG STARTEN

Sie können eine Liste mit Programmen anlegen, die beim Start der Sicheren Umgebung automatisch gestartet werden sollen.

Eine Autostart-Liste kann nur bei der Arbeit in der Sicheren Umgebung erstellt werden.

➡ *Gehen Sie folgendermaßen vor, um eine Autostart-Liste für die Sichere Umgebung anzulegen:*

1. Gehen Sie im **Startmenü** des Betriebssystems den Punkt **Programme** → **Autostart** → **Sichere Umgebung**.
2. Öffnen Sie durch Rechtsklick das Kontextmenü und wählen Sie dort den Punkt **Öffnen**.
3. Kopieren Sie die Verknüpfungen der Programme, die beim Start der Sicheren Umgebung automatisch gestartet werden sollen, in den geöffneten Ordner.

ZWISCHEN NORMALEM DESKTOP UND SICHERER UMGEBUNG WECHSELN

Sie können zum normalen Desktop wechseln, ohne die Arbeit in der Sicheren Umgebung zu beenden, und anschließend erneut zur Sicheren Umgebung umschalten. Ein Wechsel zwischen dem sicheren und normalen Desktop ist auf folgende Weise möglich:

- aus dem Hauptfenster von Kaspersky Internet Security (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 35).
- aus dem Kontextmenü von Kaspersky Internet Security (s. Abschnitt "Kontextmenü" auf S. 34).
- aus der Pop-up-Symbolleiste (s. Abschnitt "Pop-up-Symbolleiste verwenden" auf S. 148 - nur in der sicheren Umgebung verfügbar).
- mit Hilfe des Gadgets

➡ *Gehen Sie folgendermaßen vor, um aus dem Hauptfenster von Kaspersky Internet Security zum normalen Desktop zu wechseln:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Sichere Umgebung** aus.
3. Klicken Sie im folgenden Fenster auf die Schaltfläche **Normaler Desktop**.

➡ *Um aus dem Kontextmenü von Kaspersky Internet Security zum normalen Desktop zu wechseln,*

klicken Sie mit der rechten Maustaste im Infobereich der Taskleiste auf das Symbol von Kaspersky Internet Security, um das Kontextmenü zu öffnen, und wählen Sie dort den Punkt **Zurück zum normalen Desktop**.

➡ *Gehen Sie folgendermaßen vor, um aus der Popup-Symbolleiste zum normalen Desktop zu wechseln:*

1. Zeigen Sie mit der Maus auf den oberen Bildschirmbereich.
2. Klicken Sie in der Popup-Symbolleiste auf die Schaltfläche .

POPUP-SYMBOLLEISTE IN DER SICHEREN UMGEBUNG VERWENDEN

Mit der Popup-Symbolleiste der Sicheren Umgebung können folgende Aktionen ausgeführt werden:

- Sichere Umgebung beenden (s. Abschnitt "Arbeit in der Sicheren Umgebung starten und beenden" auf S. 146).
- Zurück zum normalen Desktop (s. Abschnitt "Zwischen normalem Desktop und sicherer Umgebung wechseln" auf S. 148).

➡ *Damit die Popup-Symbolleiste in der Sicheren Umgebung angezeigt wird,*

zeigen Sie mit der Maus auf den oberen Bildschirmbereich.

➡ *Gehen Sie folgendermaßen vor, um die Popup-Symbolleiste zu fixieren:*

1. Zeigen Sie mit der Maus auf den oberen Bildschirmbereich.
2. Klicken Sie in der Popup-Symbolleiste auf die Schaltfläche .

SICHERE UMGEBUNG BEREINIGEN

Bei einer Bereinigung löscht Kaspersky Internet Security die Daten, die bei der Arbeit in der Sicheren Umgebung gespeichert wurden, und stellt die veränderten Einstellungen wieder her.

Die Bereinigung wird auf dem normalen Desktop aus dem Hauptfenster von Kaspersky Internet Security ausgeführt und ist nur verfügbar, wenn die Sichere Umgebung beendet wurde.

Vergewissern Sie sich vor einer Bereinigung, dass alle Informationen, die künftig noch benötigt werden, im gemeinsamen Ordner der Sicheren Umgebung gespeichert sind. Andernfalls werden die Daten gelöscht und können nicht wiederhergestellt werden.

Gehen Sie folgendermaßen vor, um die Daten der Sicheren Umgebung zu bereinigen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Sichere Umgebung** aus.
3. Klicken Sie im folgenden Fenster Berichte auf die Schaltfläche .



4. Wählen Sie im folgenden Menü den Punkt **Sichere Umgebung leeren**.

AUF DEM DESKTOP EINE VERKNÜPFUNG FÜR DIE SICHERE UMGEBUNG ERSTELLEN

Für den Schnellstart der Sicheren Umgebung können Sie auf dem Desktop eine Verknüpfung erstellen.

Gehen Sie folgendermaßen vor, um auf dem Desktop eine Verknüpfung für den Start der Sicheren Umgebung zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Sichere Umgebung** aus.
3. Klicken Sie im folgenden Fenster Berichte auf die Schaltfläche .
4. Wählen Sie im folgenden Menü den Punkt **Verknüpfung auf Desktop erstellen**.

ÜBER DEN SICHEREN BROWSER

Der Sichere Browser dient für den Zugriff auf Systeme für Online-Banking und sonstige Webseiten, die mit vertraulichen Daten arbeiten. Sie können die Zugriffskontrolle für Online-Banking-Dienste aktivieren (s. Abschnitt "Zugriff auf Online-Banking-Dienste kontrollieren" auf S. 100), damit Banking-Webseiten automatisch erkannt werden. Außerdem können Sie den Sicheren Browser manuell starten (s. Abschnitt "Vertrauliche Daten schützen, die auf Webseiten eingegeben werden" auf S. 54).

Bei der Arbeit im Sicheren Browser gelangen eingegebene Daten und Änderungen (beispielsweise gespeicherte Cookies, Verlauf der besuchten Webseiten) nicht in das Betriebssystem und können deshalb auch nicht von Angreifern verwendet werden.

Wenn ein Browser im Sicheren Browsermodus läuft, ist sein Programmfenster grün eingerahmt.

IN DIESEM ABSCHNITT

BROWSER ALS SICHEREN BROWSER AUSWÄHLEN

Der Standard-Browser wird als Sicherer Browser verwendet. Sie können einen anderen Browser auswählen, der auf dem Computer installiert ist.

Kaspersky Internet Security unterstützt die Verwendung der folgenden Browser:

- Microsoft Internet Explorer Version 6, 7, 8 und 9
- Mozilla Firefox Version 3.x und 4.x
- Google Chrome Version 7.x und 8.x

Gehen Sie folgendermaßen vor, um einen Browser als Sicheren Browser auszuwählen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie unten im Fenster den Abschnitt **Sicherer Browser**.
3. Klicken Sie im folgenden Fenster Berichte auf die Schaltfläche .
4. Wählen Sie im folgenden Menü den Punkt **Anpassen**.
5. Dadurch wird das Fenster **Sicheren Browser anpassen** geöffnet.
6. Wählen Sie im folgenden Fenster in der Liste **Wählen Sie einen Browser als Sicheren Browser aus** den gewünschten Browser aus.
7. Klicken Sie auf **Speichern**.

SICHEREN BROWSER LEEREN

Bei der Arbeit im Sicheren Browser speichert Kaspersky Internet Security standardmäßig die Änderungen der Browser-Einstellungen und die auf Webseiten eingegebenen Daten. Aus Datenschutzgründen sollte der Sichere Browser regelmäßig bereinigt werden.

Bei einer Bereinigung löscht Kaspersky Internet Security die Daten, die bei der Arbeit im Sicheren Browser gespeichert wurden, und stellt die veränderten Einstellungen wieder her.

Vergewissern Sie sich vor einer Bereinigung, dass alle Informationen, die künftig noch benötigt werden, im gemeinsamen Ordner der sicheren Umgebung gespeichert sind. Andernfalls werden die Daten gelöscht und können nicht wiederhergestellt werden.

Anstelle einer manuellen Bereinigung können Sie die automatische Bereinigung des Sicheren Browsers aktivieren. Dadurch führt Kaspersky Internet Security automatisch eine Bereinigung aus, wenn der Sichere Browser beendet wird. Die manuelle Bereinigung ist in diesem Fall nicht verfügbar.

Gehen Sie folgendermaßen vor, um die automatische Bereinigung des Sicheren Browsers zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie unten im Fenster den Abschnitt **Sicherer Browser**.
3. Klicken Sie im folgenden Fenster Berichte auf die Schaltfläche .
4. Wählen Sie im folgenden Menü den Punkt **Anpassen**.

5. Dadurch wird das Fenster **Sicheren Browser anpassen** geöffnet.
6. Wählen Sie im folgenden Fenster unter **Erweiterte Einstellungen** die Variante **Automatische Datenbereinigung aktivieren**.
7. Klicken Sie auf **Speichern**.

AUF DEM DESKTOP EINE VERKNÜPFUNG FÜR DEN SICHEREN BROWSER ERSTELLEN

Für den Schnellstart des Sicheren Browsers können Sie auf dem Desktop eine Verknüpfung erstellen.

Gehen Sie folgendermaßen vor, um auf dem Desktop eine Verknüpfung für den Start des Sicheren Browsers zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie unten im Fenster den Abschnitt **Sicherer Browser**.
3. Klicken Sie im folgenden Fenster Berichte auf die Schaltfläche .
4. Wählen Sie im folgenden Menü den Punkt **Verknüpfung auf Desktop erstellen**.

GEMEINSAMEN ORDNER VERWENDEN

Der gemeinsame Ordner dient zum Dateiaustausch zwischen dem primärem Betriebssystem, der Sicheren Umgebung und dem Sicheren Browser. Alle Dateien, die bei der Arbeit in der Sicheren Umgebung und im Sicheren Browser in diesem Ordner gespeichert werden, stehen auf dem normalen Desktop zur Verfügung.

Der gemeinsame Ordner wird bei der Programminstallation angelegt. Der Ort des gemeinsamen Ordners variiert in Abhängigkeit des Betriebssystems:

- für das Betriebssystem Microsoft Windows XP – C:\Benutzer\All Users\Kaspersky Lab\SandboxShared
- für die Betriebssysteme Microsoft Windows Vista und Microsoft Windows 7 – C:\Benutzer\Kaspersky Lab\SandboxShared

Der Ort des gemeinsamen Ordners kann nicht geändert werden.

Der gemeinsame Ordner kann auf zwei Arten geöffnet werden:

- aus dem Programmhauptfenster (s. Abschnitt "Hauptfenster von Kaspersky Internet Security" auf S. 35)
- mit Hilfe der Verknüpfung, die durch das Symbol gekennzeichnet ist. Abhängig davon, welche Programmeinstellungen von den Entwicklern vorgegeben wurden, kann sich die Verknüpfung im Bereich "Arbeitsplatz" oder "Eigene Dokumente" des Explorers von Microsoft Windows befinden.

Gehen Sie folgendermaßen vor, um den gemeinsamen Ordner aus dem Hauptfenster von Kaspersky Internet Security zu öffnen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie unten im Fenster den Abschnitt **Sichere Umgebung oder Sicherer Browser**.
3. Klicken Sie im folgenden Fenster auf **Gemeinsamen Ordner öffnen**.

KINDERSICHERUNG

Die *Kindersicherung* kann die Aktionen unterschiedlicher Benutzer auf einem Computer und im Netzwerk kontrollieren. Die Kontrolle umfasst die Möglichkeit, den Zugriff auf Internet-Ressourcen und Programme zu beschränken, sowie die Anzeige von Berichten über die Benutzeraktionen.

Die Zahl der Kinder und Jugendlichen, die Zugang zu Computern und zum Internet besitzen, nimmt kontinuierlich zu. Durch die Risiken, mit denen die Arbeit und Kommunikation im Internet verbunden sind, ergeben sich Sicherheitsprobleme. Die wichtigsten Probleme sind:

- Besuch von Webseiten, die Zeitverlust (Chats, Online-Spiele) oder Geldverlust (Internet-Shops, Auktionen) verursachen können.
- Zugriff auf Webressourcen, die für Erwachsene bestimmt sind (z.B. Seiten, die pornografische oder extremistische Materialien enthalten, die Themen wie Waffen, Drogen und Gewalt betreffen).
- Download von infizierten Dateien.
- unverhältnismäßig lange Arbeit am Computer und damit verbundene gesundheitliche Risiken.
- Kontakte mit Fremden, die sich als Gleichaltrige ausgeben und persönliche Informationen über den Benutzer erhalten können (z.B. echter Name, Adresse, Zeiten, zu denen Kinder unbeaufsichtigt zuhause sind).

Die Kindersicherung erlaubt es, die mit der Arbeit am Computer und im Internet verbundenen Risiken zu reduzieren. Dazu dienen folgende Funktionen des Moduls:

- zeitliche Beschränkung für die Verwendung von Computer und Internet.
- Erstellen von Listen für zum Start erlaubte und verbotene Programme, sowie vorübergehende Beschränkung des Starts von erlaubten Programmen.
- Erstellen von Listen mit Webseiten, auf die der Zugriff erlaubt bzw. verboten ist. Auswahl von inhaltlichen Kategorien für Webressourcen, die nicht zur Ansicht empfohlen sind.
- Aktivieren des Modus zur sicheren Suche mit Suchmaschinen (Links zu Webseiten mit verdächtigem Inhalt werden nicht in den Suchergebnissen angezeigt).
- Beschränkung des Downloads von Dateien aus dem Internet.
- Erstellen von Listen mit Kontakten, für die die Kommunikation über Instant Messenger und in sozialen Netzwerken erlaubt oder verboten wird.
- Kontrolle des Texts von Nachrichten, die mit Instant Messengern und in sozialen Netzwerken ausgetauscht werden.
- Sendeverbot von bestimmten persönlichen Daten.
- Suche nach bestimmten Schlüsselwörtern im Nachrichtentext.

Alle Beschränkungen können einzeln aktiviert werden, wodurch sich die Kindersicherung flexibel auf unterschiedliche Benutzer anpassen lässt. Für jedes Benutzerkonto können Berichte angezeigt werden, die Ereignisse der kontrollierten Kategorien für einen bestimmten Zeitraum umfassen.

Zur Konfiguration und zur Anzeige von Berichten über die Kindersicherung müssen Benutzername und Kennwort eingegeben werden. Wenn Sie noch kein Kennwort für die Verwaltung von Kaspersky Internet Security festgelegt haben (s. Abschnitt "Kontrolle des Zugriffs auf Kaspersky Internet Security" auf S. 67), wird Ihnen beim ersten Start der Kindersicherung vorgeschlagen, dies zu tun.

IN DIESEM ABSCHNITT

KINDERSICHERUNG FÜR EINEN BENUTZER ANPASSEN

Sie können die Kindersicherung für jedes Benutzerkonto individuell aktivieren und anpassen. Dazu werden für die einzelnen Benutzer entsprechende Beschränkungen festgelegt, die z.B. vom Alter abhängig sind. Für Benutzer, deren Aktionen nicht kontrolliert werden sollen, können Sie die Kindersicherung deaktivieren.

IN DIESEM ABSCHNITT

BENUTZERKONTROLLE AKTIVIEREN UND DEAKTIVIEREN

Sie können die Kindersicherung für jedes Benutzerkonto separat aktivieren und deaktivieren. Es ist beispielsweise überflüssig, die Aktionen eines erwachsenen Benutzers, der für den Computer über Administratorrechte verfügt, zu kontrollieren. Für ihn kann die Kindersicherung deaktiviert werden. Für die übrigen Benutzer, deren Aktionen kontrolliert werden sollen, muss die Kindersicherung aktiviert und anschließend angepasst werden (z.B. standardmäßige Einstellungen aus einer Vorlage laden).

Die Kindersicherung kann auf folgende Arten aktiviert und deaktiviert werden:

- aus dem Programmhauptfenster (s. S. 35)
- aus dem Konfigurationsfenster der Kindersicherung
- aus dem Programmkonfigurationsfenster (s. S. 38)
- aus dem Kontextmenü des Programmsymbols (s. S. 34)

Aus dem Kontextmenü kann die Kindersicherung nur für das aktuelle Benutzerkonto aktiviert / deaktiviert werden.

Gehen Sie folgendermaßen vor, um die Kindersicherung für ein Benutzerkonto vom Hauptfenster aus zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf **Aktivieren**.

Gehen Sie folgendermaßen vor, um die Kindersicherung für ein Benutzerkonto vom Fenster der Kindersicherung aus zu aktivieren:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet
4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Einstellungen für Benutzerkonto**.
5. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Benutzerkontrolle aktivieren**, um die Kindersicherung für das Benutzerkonto einzuschalten.
6. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

Gehen Sie folgendermaßen vor, um die Kindersicherung für ein Benutzerkonto vom Programmkonfigurationsfenster aus zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Unterabschnitt **Kindersicherung**.
3. Wählen Sie im rechten Fensterbereich ein Benutzerkonto aus, für das die Kindersicherung aktiviert werden soll.
4. Klicken Sie oberhalb der Benutzerliste auf **Kontrollieren**.

Um die Kindersicherung für das aktuelle Benutzerkonto vom Kontextmenü aus zu aktivieren,

Wählen Sie im Kontextmenü des Programmsymbols den Punkt **Kindersicherung aktivieren**.

PARAMETER DER KINDERSICHERUNG EXPORTIEREN / IMPORTIEREN

Wenn Sie die Kindersicherung bereits für ein Benutzerkonto angepasst haben, können die Einstellungen in einer separaten Datei gespeichert werden (*Export* ausführen). Die Einstellungen können später aus dieser Datei geladen werden, um die Komponente schnell anzupassen (*Import* ausführen). Außerdem können die Einstellungen, die für die Kontrolle eines anderen Benutzerkontos gelten, übernommen oder es kann eine Konfigurationsvorlage verwendet werden (eine vordefinierte Auswahl von Regeln für unterschiedliche Benutzertypen, die sich an Alter, Erfahrung und anderen Merkmalen orientieren).

Nachdem eine Auswahl von Einstellungen für ein Benutzerkonto übernommen wurde, können die Werte geändert werden. Dies hat keinen Einfluss auf die Werte in der Datei, aus der die Einstellungen importiert wurden.

Gehen Sie folgendermaßen vor, um die Einstellungen in einer Datei zu speichern:

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.

3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet

4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Einstellungen für Benutzerkonto**.

5. Klicken Sie rechts im Fenster unter **Einstellungen verwalten** auf **Speichern** und speichern Sie die Konfigurationsdatei.

➡ *Gehen Sie folgendermaßen vor, um Einstellungen aus einer Datei zu laden:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.

3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf **Aktivieren**.

   Das Fenster **Kindersicherung** wird geöffnet

4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Einstellungen für Benutzerkonto**.

5. Klicken Sie rechts im Fenster unter **Einstellungen verwalten** auf **Laden**.

6. Wählen Sie im folgenden Fenster **Einstellungen für Kindersicherung laden** die Variante **Konfigurationsdatei** und geben Sie den Ort der Datei an.

➡ *Gehen Sie folgendermaßen vor, um die Einstellungen eines Benutzerkontos zu übernehmen:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.

3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf **Aktivieren**.

   Das Fenster **Kindersicherung** wird geöffnet

4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Einstellungen für Benutzerkonto**.

5. Klicken Sie rechts im Fenster unter **Einstellungen verwalten** auf **Laden**.

6. Wählen Sie im folgenden Fenster **Einstellungen für Kindersicherung laden** die Variante **Anderer Benutzer** und geben Sie das Benutzerkonto an, dessen Einstellungen verwendet werden sollen.

➡ *Gehen Sie folgendermaßen vor, um eine Konfigurationsvorlage zu verwenden:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.

3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf **Aktivieren**.

   Das Fenster **Kindersicherung** wird geöffnet

4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Einstellungen für Benutzerkonto**.

5. Klicken Sie rechts im Fenster unter **Einstellungen verwalten** auf **Laden**.

6. Wählen Sie im folgenden Fenster **Einstellungen für Kindersicherung laden** die Variante **Vorlage** und geben Sie die Vorlage an, deren Einstellungen verwendet werden sollen.

DARSTELLUNG EINES BENUTZERKONTOS IN KASPERSKY INTERNET SECURITY

Sie können ein Alias und ein Bild wählen, die in Kaspersky Internet Security für ein Benutzerkonto angezeigt werden sollen.

➡ *Gehen Sie folgendermaßen vor, um ein Alias und ein Bild für ein Benutzerkonto festzulegen:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet
4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Einstellungen für Benutzerkonto**.
5. Geben Sie rechts im Fenster im Feld **Alias** ein Benutzeralias ein.
6. Wählen Sie im Block **Bild** ein Bild für das Benutzerkonto aus.
7. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

ARBEITSZEIT AUF DEM COMPUTER

Sie können einen Zeitplan einrichten, der den Zugriff eines Benutzers auf den Computer reguliert (Wochentage und Zeiträume im Verlauf eines Tages). Außerdem kann die tägliche Arbeitszeit auf dem Computer begrenzt werden.

➡ *Gehen Sie folgendermaßen vor, um die Arbeitsdauer für den Computer zu beschränken:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet
4. Öffnen Sie die Registerkarte **Einstellungen** und wählen Sie dann links im Fenster den Abschnitt **Verwendung des Computers**.
5. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
6. Legen Sie die zeitlichen Beschränkungen für die Verwendung des Computers fest.
7. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

ARBEITSZEIT IM INTERNET

Sie können die Zeit, die ein Benutzer im Internet verbringen darf, beschränken. Dazu lässt sich ein Zeitplan für den Internetzugriff einstellen (Wochentage und Zeiträume im Verlauf eines Tages, in denen der Zugriff erlaubt oder verboten ist). Außerdem kann die tägliche Verwendungsdauer für das Internet begrenzt werden.

➡ *Gehen Sie folgendermaßen vor, um die Arbeitsdauer im Internet zu beschränken:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet
4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Verwendung des Internets**.
5. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
6. Legen Sie die zeitlichen Beschränkungen für die Verwendung des Internets fest.
7. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

START VON PROGRAMMEN

Sie können den Start bestimmter Programme erlauben oder verbieten. Außerdem kann der Start erlaubter Programme zeitlich eingeschränkt werden.

➡ *Gehen Sie folgendermaßen vor, um den Start von Programmen einzuschränken:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet
4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Start von Programmen**.
5. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
6. Erstellen Sie die Listen für Programme, deren Start erlaubt bzw. verboten ist, und legen Sie einen Zeitplan für die Verwendung von erlaubten Programmen fest.
7. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

BESUCH VON WEBSEITEN

Sie können den Zugriff auf Webseiten in Abhängigkeit von ihrem Inhalt beschränken. Dazu können Kategorien von Webseiten gewählt werden, auf die der Zugriff blockiert werden soll. Außerdem kann eine Liste von Ausnahmen angelegt werden.

Sie können den *Modus für sichere Suche* aktivieren, der zum Einsatz kommt, wenn ein Benutzer mit Suchmaschinen arbeitet. Bestimmte Suchmaschinen versuchen, ihre Nutzer vor unzulässigen Inhalten auf Webressourcen zu schützen. Dazu werden Webseiten bei der Indizierung auf Schlüsselwörter und Phrasen, Adressen und Ressourcenkategorien hin analysiert. Wenn der Modus für sichere Suche aktiviert ist, werden Webseiten, die unerwünschten Kategorien angehören (Pornografie, Drogen, Gewalt und sonstige Materialien, die nicht für Minderjährige geeignet sind), von den Suchergebnissen ausgeschlossen.

Die Kindersicherung erlaubt es, den Modus für sichere Suche gleichzeitig für folgende Suchmaschinen zu aktivieren:

- Google
- Bing

Gehen Sie folgendermaßen vor, um den Zugriff auf Webseiten zu beschränken:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet
4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Besuch von Webseiten**.
5. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
6. Wählen Sie im Block **Webseiten verbieten** einen Modus für den Zugriff auf Webseiten aus:
   - Wenn der Zugriff auf bestimmte Webseiten-Kategorien verboten werden soll, wählen Sie die Variante **Folgende Webseiten-Kategorien verbieten** und aktivieren Sie die Kontrollkästchen für die Webseiten-Kategorien, auf die der Zugriff blockiert werden soll.

     Wenn der Zugriff auf bestimmte Webseiten erlaubt werden soll, die einer gesperrten Kategorie angehören, klicken Sie auf **Ausnahmen**, fügen Sie die betreffenden Webadressen zur Ausnahmeliste hinzu und weisen Sie ihnen den Status **Erlaubt** zu.
   - Wenn Sie eine Liste mit erlaubten Webseiten anlegen und den Zugriff auf alle übrigen Webseiten verbieten möchten, wählen Sie die Variante **Besuch aller Webseiten verbieten, außer wenn durch Ausnahmeliste erlaubt**, klicken Sie auf **Ausnahmen**, fügen Sie die betreffenden Webadressen zur Ausnahmeliste hinzu und weisen Sie ihnen den Status **Erlaubt** zu.
   - Wenn Sie den Zugriff auf bestimmte Webseiten verbieten möchten, klicken Sie auf **Ausnahmen**, fügen Sie die betreffenden Webadressen zur Ausnahmeliste hinzu und weisen Sie ihnen den Status **Verboten** zu.
7. Aktivieren Sie das Kontrollkästchen **Sichere Suche aktivieren**, um den Modus für die sichere Suche zu aktivieren.
8. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

DOWNLOAD VON DATEIEN AUS DEM INTERNET

Sie können angeben, welche Dateitypen ein Benutzer aus dem Internet herunterladen darf.

Gehen Sie folgendermaßen vor, um den Download von Dateien aus dem Internet einzuschränken:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet
4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Download von Dateien**.

5. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
6. Wählen Sie die Dateikategorien, deren Download erlaubt ist.
7. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

KORRESPONDENZ ÜBER INSTANT MESSENGER

Die Kontrolle der Konversationen mit Programmen zum Nachrichtensofortversand (Instant Messenger) umfasst die Kontrolle von erlaubten Kontakten, das Blockieren der Konversationen mit verbotenen Kontakten, sowie die Kontrolle des Nachrichteninhalts. Sie können Listen mit erlaubten und verbotenen Kontakten anlegen, Schlüsselwörter festlegen, auf deren Vorhandensein die Nachrichten überprüft werden, und persönliche Informationen, die nicht gesendet werden dürfen, angeben.

Wenn Konversationen mit einem Kontakt verboten sind, werden alle Nachrichten, die sich an diesen Kontakt richten oder von ihm stammen, blockiert. Informationen über blockierte Nachrichten und das Vorhandensein von Schlüsselwörtern in Nachrichten werden protokolliert. Im Bericht sind auch die Nachrichtentexte für jeden Kontakt enthalten.

Die Konversationskontrolle besitzt folgende Einschränkungen:

- Wenn ein Instant Messenger gestartet wurde, bevor die Kindersicherung aktiviert wurde, erfolgt die Konversationskontrolle erst nach einem Neustart des Instant Messengers.
- Bei Verwendung eines HTTP-Proxys werden die Konversationen nicht kontrolliert.

Die aktuelle Version der Kindersicherung bietet die Kontrolle für folgende Instant Messenger:

- ICQ
- QIP
- Windows Live Messenger (MSN)
- Yahoo Messenger
- GoogleTalk
- mIRC
- Mail.Ru Agent
- Psi
- Miranda
- Digsby
- Pidgin
- Qnext
- SIM
- Trilian
- Xchat
- Instantbird
- RnQ

- MSN
- Jabber

Manche Instant Messenger wie z.B. Yahoo! Messenger und Google Talk verwenden eine geschützte Verbindung. Um den Datenverkehr dieser Programme zu untersuchen, muss die Untersuchung von geschützten Verbindungen aktiviert werden (s. S. 123).

Gehen Sie folgendermaßen vor, um Konversationen zu beschränken, die über Instant Messenger erfolgen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet
4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **IM-Konversationen**.
5. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
6. Legen Sie die Listen für erlaubte und verbotene Kontakte an.
   a. Klicken Sie in der Liste **Kontakte** auf **Kontakt hinzufügen**.
   b. Wählen Sie im folgenden Fenster **Neuer Kontakt** in der Liste einen Kontakt aus oder fügen Sie ihn manuell hinzu.
7. Aktivieren Sie das Kontrollkästchen **Konversationen mit Kontakten verbieten, die nicht auf der Liste stehen**, wenn die Kommunikation nur mit jenen Kontakten erlaubt werden soll, die in der Liste den Status **Erlaubt** besitzen.
8. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

KONVERSATIONEN IN SOZIALEN NETZWERKEN

Die Kontrolle der Konversationen über soziale Netzwerke umfasst die Kontrolle von erlaubten Kontakten, das Blockieren der Konversationen mit verbotenen Kontakten, sowie die Kontrolle des Nachrichteninhalts. Sie können Listen mit erlaubten und verbotenen Kontakten anlegen, Schlüsselwörter festlegen, auf deren Vorhandensein die Nachrichten überprüft werden, und persönliche Informationen, die nicht gesendet werden dürfen, angeben.

Wenn Konversationen mit einem Kontakt verboten sind, werden alle Nachrichten, die sich an diesen Kontakt richten oder von ihm stammen, blockiert. Informationen über blockierte Nachrichten und das Vorhandensein von Schlüsselwörtern in Nachrichten werden protokolliert. Im Bericht sind auch die Nachrichtentexte für jeden Kontakt enthalten.

Manche sozialen Netzwerke wie z.B. Twitter verwenden eine geschützte Verbindung. Um den Datenverkehr dieser Netzwerke zu untersuchen, muss die Untersuchung von geschützten Verbindungen aktiviert werden (s. S. 123).

Gehen Sie folgendermaßen vor, um Konversationen zu beschränken, die über soziale Netzwerke erfolgen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet

4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Soziale Netzwerke**.
5. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
6. Legen Sie die Listen für erlaubte und verbotene Kontakte an.

   Es kann keine Liste angelegt werden, wenn Kaspersky Internet Security noch nicht genügend Daten über die Verwendung von sozialen Netzwerken gesammelt hat.

   a. Klicken Sie in der Liste **Kontakte** auf **Kontakt hinzufügen**.
   b. Wählen Sie im folgenden Fenster **Neuer Kontakt** in der Liste einen Kontakt aus oder fügen Sie ihn manuell hinzu.
7. Aktivieren Sie das Kontrollkästchen **Konversationen mit Kontakten verbieten, die nicht auf der Liste stehen**, wenn die Kommunikation nur mit jenen Kontakten erlaubt werden soll, die in der Liste den Status **Erlaubt** besitzen.
8. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

SENDEN VERTRAULICHER INFORMATIONEN

Sie können verbieten, dass Daten, die persönliche Informationen enthalten, über Instant Messenger, soziale Netzwerke und beim Senden von Daten über Webseiten verschickt werden. Dafür ist es erforderlich, eine Liste mit Einträgen anzulegen, die vertrauliche Informationen enthalten (z.B. Adresse, Telefonnummer usw.).

Versuche zum Senden von Daten aus dieser Liste werden blockiert und es werden Informationen über blockierte Nachrichten im Bericht aufgezeichnet.

Gehen Sie folgendermaßen vor, um das Senden von vertraulichen Informationen zu verbieten:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet
4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Persönliche Daten**.
5. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
6. Legen Sie eine Liste mit persönlichen Daten an, die nicht gesendet werden dürfen.
   a. Klicken Sie in der Liste **Persönliche Daten** auf **Hinzufügen**.
   b. Geben Sie im folgenden Fenster **Persönliche Daten** die Informationen an, die nicht gesendet werden dürfen.
7. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

SUCHE NACH SCHLÜSSELWÖRTERN

Sie können überwachen, ob in den Konversationen eines Benutzers, die über Instant Messenger, soziale Netzwerke und beim Senden von Daten über Webseiten erfolgen, bestimmte Wörter oder Phrasen vorkommen.

Das Vorhandensein von festgelegten Schlüsselwörtern in ausgetauschten Nachrichten wird protokolliert.

Wenn die Konversationskontrolle für Instant Messenger und soziale Netzwerke oder die Kontrolle für den Besuch von Webseiten deaktiviert ist, erfolgt keine Suche nach Schlüsselwörtern.

Gehen Sie folgendermaßen vor, um zu überwachen, ob in Konversationen und in gesendeten Daten bestimmte Wörter vorkommen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet
4. Wählen Sie die Registerkarte **Einstellungen** und wählen Sie auf der linken Fensterseite den Abschnitt **Schlüsselwörter**.
5. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Kontrolle aktivieren**.
6. Legen Sie eine Liste mit Schlüsselwörtern an, die in Konversationen und in gesendeten Daten überwacht werden sollen:
   a. Klicken Sie in der Liste **Schlüsselwörter** auf **Hinzufügen**.
   b. Geben Sie im folgenden Fenster **Schlüsselwort** die zu überwachenden Wörter und Phrasen an.
7. Klicken Sie auf **Übernehmen**, um die vorgenommenen Änderungen zu speichern.

BERICHTE ÜBER DIE AKTIONEN EINES BENUTZERS ANZEIGEN

Sie können Berichte über die Aktionen jedes Benutzers ansehen, für den die Kindersicherung aktiviert wurde. Es sind Berichte für jede Kategorie der kontrollierten Ereignisse verfügbar.

Gehen Sie folgendermaßen vor, um einen Bericht über die Aktionen eines kontrollierten Benutzers anzuzeigen:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Kindersicherung**.
3. Klicken Sie im folgenden Fenster im Block des Benutzerkontos auf das Symbol für **Einstellungen**.

   Das Fenster **Kindersicherung** wird geöffnet
4. Wählen Sie die Registerkarte **Berichte**.
5. Wählen Sie links im Fenster einen Abschnitt mit dem Namen einer Kategorie für kontrollierte Aktionen oder Inhalte aus (z.B. **Verwendung des Internet** oder **Persönliche Daten**).

   Auf der rechten Fensterseite befindet sich ein Bericht über die kontrollierten Aktionen und Inhalte.

VERTRAUENSWÜRDIGE ZONE

Die *vertrauenswürdige Zone* ist eine Liste von Objekten, die nicht vom Programm kontrolliert werden. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz, den Kaspersky Internet Security bietet.

Die vertrauenswürdige Zone wird auf Basis einer Liste der vertrauenswürdigen Programme (s. Abschnitt "Liste mit vertrauenswürdigen Programmen erstellen" auf S. 163) und der Ausnahmeregeln (s. Abschnitt "Ausnahmeregeln erstellen" auf S. 164) eingerichtet, wobei die Besonderheiten der Objekte, mit denen Sie arbeiten, sowie der Programme, die auf Ihrem Computer installiert sind, zu berücksichtigen sind. Die Aufnahme von Objekten in die vertrauenswürdige Zone kann beispielsweise erforderlich sein, wenn Kaspersky Internet Security den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt / Programm absolut unschädlich ist.

Wenn Sie beispielsweise die Objekte, die von dem standardmäßigen Microsoft Windows-Programm Editor verwendet werden, für ungefährlich und ihre Untersuchung für nicht erforderlich halten, Sie diesem Programm also vertrauen, dann fügen Sie das Programm Editor zur Liste der vertrauenswürdigen Programme hinzu, um die Objekte, die von diesem Prozess benutzt werden, von der Untersuchung auszuschließen.

Außerdem können bestimmte Aktionen, die als gefährlich klassifiziert werden, im Rahmen der Funktionalität bestimmter Programme ungefährlich sein. So ist das Abfangen eines über die Tastatur eingegebenen Texts für Programme zum automatischen Umschalten der Tastaturbelegung (z.B. Punto Switcher) eine normale Aktion. Um die Besonderheit solcher Programme zu berücksichtigen und die Kontrolle ihrer Aktivität abzuschalten, empfehlen wir, sie in die Liste der vertrauenswürdigen Anwendungen aufzunehmen.

Wenn ein Programm der vertrauenswürdigen Liste hinzugefügt wird, werden die Datei- und Netzwerkaktivität dieses Programms (einschließlich verdächtiger Aktivität) sowie seine Zugriffe auf die Systemregistrierung nicht kontrolliert. Zugleich werden die ausführbare Datei und der Prozess eines vertrauenswürdigen Programms weiterhin auf Viren untersucht. Um ein Programm vollständig von der Untersuchung auszuschließen, müssen die Ausnahmeregeln verwendet werden.

Durch das Ausschließen vertrauenswürdiger Programme von der Untersuchung lassen sich Kompatibilitätsprobleme von Kaspersky Internet Security mit anderen Programmen vermeiden (beispielsweise Probleme einer doppelten Untersuchung des Netzwerkverkehrs eines anderen Computers durch Kaspersky Internet Security und durch ein anderes Antiviren-Programm). Außerdem lässt sich dadurch die Leistungsfähigkeit des Computers erhöhen, was speziell bei der Verwendung von Serverprogrammen wichtig ist.

Die Ausnahmeregeln der vertrauenswürdigen Zone gewährleisten ihrerseits die Möglichkeit, mit legalen Programmen zu arbeiten, die von Angreifern für die Schädigung des Computers oder Ihrer Daten verwendet werden können. Solche Programme haben zwar selbst keine schädlichen Funktionen, können aber von Schadprogrammen als Hilfskomponenten missbraucht werden. Zu dieser Kategorie gehören beispielsweise Programme zur Remote-Verwaltung, IRC-Clients, FTP-Server, unterschiedliche Hilfsprogramme zum Beenden von Prozessen und zum Verstecken ihrer Arbeit, Tastaturspione, Programme zur Kennwortermittlung, Programme zur automatischen Einwahl u.a. Derartige Programme können aufgrund der Arbeit von Kaspersky Internet Security gesperrt werden. Um das Sperren zu verhindern, können für die verwendeten Programme Ausnahmeregeln erstellt werden.

Eine *Ausnahmeregel* ist eine Kombination von Bedingungen, bei deren Erfüllung ein Objekt nicht von Kaspersky Internet Security untersucht wird. In allen übrigen Fällen wird dieses Objekt von allen Schutzkomponenten mit den festgelegten Parametern untersucht.

Die Ausnahmeregeln der vertrauenswürdigen Zone können von mehreren Programmkomponenten (z.B. Datei-Anti-Virus (s. Abschnitt "Datei-Anti-Virus" auf S. 81), Mail-Anti-Virus (s. Abschnitt "Mail-Anti-Virus" auf S. 88), Web-Anti-Virus (s. Abschnitt "Web-Anti-Virus" auf S. 93)) sowie bei der Ausführung von Untersuchungsaufgaben verwendet werden.

IN DIESEM ABSCHNITT

LISTE MIT VERTRAUENSWÜRDIGEN PROGRAMMEN ERSTELLEN

Kaspersky Internet Security untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden sollen, und kontrolliert die Aktivität aller Programme und den von ihnen erzeugten Netzwerkverkehr. Die Programme der vertrauenswürdigen Liste werden von Kaspersky Internet Security von der Untersuchung ausgeschlossen.

➡ *Gehen Sie folgendermaßen vor, um ein Programm zur Liste der vertrauenswürdigen Programme hinzuzufügen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Gefahren und Ausnahmen**.
3. Klicken Sie im Block **Ausnahmen** auf **Einstellungen...**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Vertrauenswürdige Programme** auf die Schaltfläche **Hinzufügen**, um das Menü zur Programmauswahl zu öffnen.
5. Wählen Sie ein Programm aus der Dropdown-Liste **Programme** oder gehen Sie auf den Punkt **Durchsuchen**, um den Pfad der ausführbaren Datei des entsprechenden Programms anzugeben.
6. Aktivieren Sie im folgenden Fenster **Ausnahmen für das Programm** die Kontrollkästchen für die Arten der Programmaktivität, die nicht untersucht werden sollen.

AUSNAHMEREGELN ERSTELLEN

Falls Sie in Ihrer Arbeit Programme benutzen, die von Kaspersky Internet Security als legal eingestuft werden und von Angreifern zur Schädigung des Computers oder Ihrer Daten verwendet werden können, empfehlen wir Ihnen, für diese Ausnahmen einzurichten.

➡ *Gehen Sie folgendermaßen vor, um eine Ausnahmeregel zu erstellen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Gefahren und Ausnahmen**.
3. Klicken Sie im Block **Ausnahmen** auf **Einstellungen...**.
4. Klicken Sie im folgenden Fenster auf der Registerkarte **Regeln für Ausnahmen** auf **Hinzufügen**.
5. Geben Sie im folgenden Fenster **Ausnahmeregel** die Parameter der Ausnahmeregel an.

LEISTUNG UND KOMPATIBILITÄT MIT ANDEREN PROGRAMMEN

Die Leistungseinstellungen für Kaspersky Internet Security umfassen das Spektrum der erkennbaren Bedrohungen sowie Energieverbrauch und benötigte Computerressourcen.

Kaspersky Internet Security erlaubt es, unterschiedliche Bedrohungskategorien (s. Abschnitt "Kategorien der erkennbaren Bedrohungen wählen" auf S. 165) zu wählen, die das Programm erkennen soll.

Bei der Arbeit auf einem Laptop besitzt der Energieverbrauch, der von Programmen verursacht wird, eine besondere Bedeutung. Eine Virenuntersuchung des Computers und das Datenbank-Update beanspruchen erhebliche Ressourcen. Ein spezieller Modus für die Arbeit von Kaspersky Internet Security auf einem Laptop (s. Abschnitt "Energiesparen im Akkubetrieb" auf S. 165) schiebt geplante Untersuchungs- und Updateaufgaben automatisch auf, wenn die Stromversorgung von einer Batterie erfolgt, und spart dadurch Akkustrom. Der Modus zur Untersuchung im Computerleerlauf (s. Abschnitt "Aufgabenstart im Hintergrundmodus" auf S. 166) erlaubt es, ressourcenaufwändige Aufgaben dann zu starten, wenn der Computer nicht verwendet wird.

Der von Kaspersky Internet Security verursachte Verbrauch von Computerressourcen kann sich auf die Performance anderer Programme auswirken. Um bei der gleichzeitigen Arbeit mit anderen Programmen Probleme durch eine hohe Last auf Prozessor und Laufwerk-Subsysteme zu vermeiden, kann Kaspersky Internet Security Untersuchungsaufgaben anhalten und Ressourcen für andere Programme freigeben (s. Abschnitt "Verteilung der Computerressourcen bei der Virensuche" auf S. 166), die auf dem Computer laufen.

Im Modus Profil für Spiele (s. S. 167) wird die Anzeige von Meldungen über die Aktivität von Kaspersky Internet Security automatisch deaktiviert, wenn andere Programme im Vollbildmodus gestartet werden.

Der erweiterte Desinfektionsvorgang, der für den Fall einer aktiven Infektion vorgesehen ist, erfordert einen obligatorischen Neustart des Computers, was sich ebenfalls auf die Arbeit anderer Programme auswirken kann. Bei Bedarf können Sie die Verwendung der Technologie zur Desinfektion aktiver Infektionen (s. S. 166) deaktivieren, um eine unerwünscht hohe Auslastung des Computers zu vermeiden.

IN DIESEM ABSCHNITT

KATEGORIEN DER ERKENNBAREN BEDROHUNGEN WÄHLEN

Die Bedrohungen, die von Kaspersky Internet Security erkannt werden, sind nach unterschiedlichen Merkmalen in Kategorien angeordnet. Viren, trojanische Programme und schädliche Tools werden immer vom Programm erkannt. Diese Programme können Ihrem Computer ernsthaften Schaden zufügen. Zur Steigerung der Computersicherheit lässt sich die Liste der zu erkennenden Bedrohungen durch Aktivierung der Kontrolle des Verhaltens legaler Programme erweitern, die von Angreifern zur Schädigung des Computers oder Ihrer Daten verwendet werden können.

➧ *Gehen Sie folgendermaßen vor, um die Kategorien erkennbare Bedrohungen auszuwählen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Gefahren und Ausnahmen**.
3. Klicken Sie auf der rechten Fensterseite auf die unterhalb der Liste **Erkennung folgender Bedrohungstypen aktiviert** angeordnete Schaltfläche **Einstellungen**.
4. Aktivieren Sie im folgenden Fenster **Bedrohungen** die Kontrollkästchen für die Bedrohungen, die erkannt werden sollen.

ENERGIESPAREN IM AKKUBETRIEB

Um sparsam mit der Batterie eines Laptops umzugehen, können Sie Aufgaben zur Virensuche und zum Update nach Zeitplan aufschieben. Bei Bedarf können Sie Kaspersky Internet Security auf Befehl aktualisieren oder die Virenuntersuchung manuell starten.

➧ *Gehen Sie folgendermaßen vor, um den Energiesparmodus bei Akkubetrieb zu aktivieren:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Energiesparen**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Geplante Untersuchungsaufgaben bei Akkubetrieb nicht starten**.

AKTIVE DESINFEKTION

Moderne Schadprogramme können in die tiefste Ebene des Betriebssystems eindringen, wodurch es praktisch unmöglich wird, sie zu löschen. Wenn Kaspersky Internet Security eine schädliche Aktivität im System erkennt, bietet er an, Technologie zur Desinfektion aktiver Infektionen zu verwenden, durch die die Bedrohung neutralisiert und vom Computer gelöscht wird.

Zum Abschluss der Desinfektion einer aktiven Infektion erfolgt ein obligatorischer Neustart des Computers. Nach dem Neustart des Computers wird empfohlen, eine vollständige Virenuntersuchung zu starten (s. Abschnitt "Vollständige Virenuntersuchung des Computers ausführen" auf S. 51).

➧ *Gehen Sie folgendermaßen vor, damit Kaspersky Internet Security die Technologie zur Desinfektion aktiver Infektionen anwendet:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Kompatibilität**.
3. Aktivieren Sie das Kontrollkästchen **Technologie zur aktiven Desinfektion verwenden**.

VERTEILUNG DER COMPUTERRESSOURCEN BEI DER VIRENSUCHE

Das Ausführen von Untersuchungsaufgaben erhöht die Auslastung des Prozessors und der Laufwerke und verlangsamt dadurch die Arbeit anderer Programme. In der Grundeinstellung hält Kaspersky Internet Security beim Eintreten dieser Situation die Ausführung von Untersuchungsaufgaben an und gibt Systemressourcen für Benutzeranwendungen frei.

Allerdings existiert eine Reihe von Programmen, die gestartet werden, wenn Prozessorressourcen frei werden, und im Hintergrundmodus arbeiten. Wenn die Untersuchung von der Arbeit solcher Programme unabhängig sein soll, sollten ihnen keine Systemressourcen überlassen werden.

➧ *Gehen Sie folgendermaßen vor, damit Kaspersky Internet Security die Untersuchungsaufgaben zurückstellt, wenn sie die Arbeit anderer Programme verlangsamen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Kompatibilität**.
3. Aktivieren Sie das Kontrollkästchen **Ressourcen für andere Programme freigeben**.

AUFGABENSTART IM HINTERGRUNDMODUS

Um eine optimale Auslastung der Computerressourcen zu erreichen, führt Kaspersky Internet Security eine regelmäßige Rootkit-Suche im Hintergrundmodus sowie den Start von ressourcenintensiven Aufgaben bei Computerleerlauf aus.

Die regelmäßige Rootkit-Suche wird ausgeführt, während Sie mit dem Computer arbeiten. Die Suche dauert maximal 5 Minuten und erfordert minimale Computerressourcen.

Zu den Aufgaben die bei Leerlauf des Computers gestartet werden können, zählen:

- automatisches Update der Antiviren-Datenbanken und Programm-Module
- Untersuchung des Arbeitsspeichers, der Autostart-Objekte und der Systempartition

Aufgaben werden bei Computerleerlauf gestartet, wenn der Computer vom Benutzer gesperrt wurde oder der Bildschirmschoner länger als 5 Minuten angezeigt wird.

Wenn der Computer im Batteriebetrieb arbeitet, werden im Computerleerlauf keine Aufgaben gestartet.

Der Fortschritt von Aufgaben, die im Hintergrundmodus gestartet wurden, wird in der Aufgabenübersicht angezeigt (s. Abschnitt "Untersuchungsaufgaben verwalten. Aufgabenübersicht" auf S. 76).

IN DIESEM ABSCHNITT

ROOTKIT-SUCHE IM HINTERGRUNDMODUS

Standardmäßig führt Kaspersky Internet Security eine regelmäßige Rootkit-Suche aus. Bei Bedarf können Sie die Rootkit-Suche deaktivieren.

Gehen Sie folgendermaßen vor, um die regelmäßige Rootkit-Suche zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Untersuchung des Computers** den Abschnitt **Allgemeine Einstellungen**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Regelmäßige Rootkit-Suche ausführen**.

UNTERSUCHUNG BEI COMPUTERLEERLAUF

Der erste Schritt für den Start von Aufgaben, die bei Computerleerlauf ausgeführt werden, besteht in einer Aktualitätsprüfung der Datenbanken und Programm-Module. Wenn sich daraus ergibt, dass eine Aktualisierung erforderlich ist, wird die Aufgabe zum automatischen Update gestartet. Beim zweiten Schritt werden Datum und Status der letzten Aufgabenausführung bei Computerleerlauf geprüft. Wenn die Aufgabe bei Computerleerlauf noch nicht gestartet wurde, länger als 7 Tage nicht ausgeführt wurde oder abgebrochen wurde, wird die Aufgabe zur Untersuchung des Arbeitsspeichers, der Autostart-Objekte und der Systemregistrierung gestartet.

Die Untersuchung bei Computerleerlauf wird mit einer tief gehenden heuristischen Analyse ausgeführt, wodurch sich eine hohe Wahrscheinlichkeit für den Fund von versteckten Bedrohungen ergibt.

Die Aufgabe bei Computerleerlauf wird abgebrochen, wenn der Benutzer seine Arbeit fortsetzt. Dabei wird festgehalten, an welcher Stelle die Aufgabe abgebrochen wurde, um sie beim nächsten Mal dort fortzusetzen.

Wenn die Aufgabenausführung bei Computerleerlauf abgebrochen wurde, während ein Update heruntergeladen wurde, so wird die Aktualisierung beim nächsten Mal neu gestartet.

Gehen Sie folgendermaßen vor, um die Ausführung von Aufgaben bei Computerleerlauf zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite unter **Untersuchung des Computers** den Abschnitt **Allgemeine Einstellungen**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Untersuchung bei Computerleerlauf ausführen**.

IM VOLLBILDMODUS ARBEITEN. PROFIL FÜR SPIELE

Die Verwendung bestimmter Programme (insbesondere von Computerspielen) im Vollbildmodus ist für die Kompatibilität mit einigen Funktionen von Kaspersky Internet Security problematisch. In diesem Modus sind beispielsweise Meldungsfenster unangebracht. Teilweise nehmen solche Programme auch erhebliche Systemressourcen in Anspruch,

sodass die Ausführung einer Aufgabe von Kaspersky Internet Security zu einer Verlangsamung dieser Programme führen kann.

Damit der Benutzer nicht jedes Mal, wenn er in den Vollbildmodus wechselt, manuell die Benachrichtigungen deaktivieren und Aufgaben anhalten muss, bietet Kaspersky Internet Security die Möglichkeit, diese Einstellungen mit Hilfe eines Profils für Spiele vorübergehend zu ändern. Wenn das Spiele-Profil aktiviert wird, werden beim Wechsel in den Vollbildmodus automatisch die Einstellungen aller Komponenten so geändert, dass eine optimale Arbeit in diesem Modus gewährleistet ist. Bei Verlassen des Vollbildmodus werden für die Einstellungen des Programms die Werte wiederhergestellt, die vor dem Wechsel in den Vollbildmodus eingestellt waren.

Gehen Sie folgendermaßen vor, um die Verwendung des Profils für Spiele zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Profil für Spiele**.
3. Aktivieren Sie das Kontrollkästchen **Profil für Spiele verwenden** und geben Sie darunter im Block **Einstellungen für Profil** die erforderlichen Einstellungen für die Verwendung des Spiele-Profils an.

SELBSTSCHUTZ FÜR KASPERSKY INTERNET SECURITY

Da Kaspersky Internet Security für die Sicherheit des Computers vor schädlichen Programmen verantwortlich ist, versuchen bestimmte Schadprogramme, die auf den Computer gelangen, die Arbeit von Kaspersky Internet Security zu blockieren oder ihn vom Computer zu löschen.

Die Stabilität des Schutzes Ihres Computers wird in Kaspersky Internet Security durch Mechanismen zum Selbstschutz und zum Schutz vor externer Steuerung realisiert.

Der Selbstschutz für Kaspersky Internet Security verhindert, dass seine Dateien auf der Festplatte, Prozesse im Speicher und Einträge in der Registrierung verändert oder gelöscht werden. Der Schutz vor externer Steuerung ermöglicht das Blockieren aller Versuche, die Programmdienste von einem entfernten Standort zu verwalten.

Für 64-Bit-Betriebssysteme und für Microsoft Windows Vista steht der Selbstschutzmechanismus von Kaspersky Internet Security nur im Hinblick auf Veränderungen oder Löschen von eigenen Dateien auf der Festplatte und Veränderungen oder Löschen von Einträgen in der Systemregistrierung zur Verfügung.

IN DIESEM ABSCHNITT

SELBSTSCHUTZ AKTIVIEREN UND DEAKTIVIEREN

Der Selbstschutz von Kaspersky Internet Security ist standardmäßig aktiviert. Bei Bedarf können Sie den Selbstschutz deaktivieren.

Gehen Sie folgendermaßen vor, um den Selbstschutz von Kaspersky Internet Security zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Selbstschutz**.
3. Deaktivieren Sie auf der rechten Seite des Fensters das Kontrollkästchen **Selbstschutz aktivieren**.

SCHUTZ VOR EXTERNER STEUERUNG

Standardmäßig ist der Schutz vor externer Steuerung aktiviert. Bei Bedarf können Sie den Schutz deaktivieren.

Wenn der Schutz vor externer Steuerung aktiviert ist, kann es vorkommen, dass gleichzeitig Programme zur Remote-Administration eingesetzt werden sollen (z.B. RemoteAdmin). Um diese Programme zu aktivieren, fügen Sie sie zur Liste der vertrauenswürdigen Programme (s. Abschnitt "Vertrauenswürdige Zone" auf S. 162) hinzu, und aktivieren Sie die Einstellung **Programmaktivität nicht kontrollieren**.

Gehen Sie folgendermaßen vor, um den Schutz vor externer Steuerung zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Selbstschutz**.
3. Deaktivieren Sie im Block **Externe Steuerung** das Kontrollkästchen **Option zur externen Steuerung des Systemdienstes deaktivieren**.

QUARANTÄNE UND BACKUP

Quarantäne ist ein spezieller Speicher, in den Dateien verschoben werden, die möglicherweise von Viren infiziert oder im Augenblick des Funds irreparabel sind.

Eine verdächtige Datei kann während der Virensuche sowie bei der Ausführung von Datei-Anti-Virus, Mail-Anti-Virus und Proaktiver Schutz gefunden und in die Quarantäne verschoben werden.

Dateien werden in folgenden Fällen in die Quarantäne verschoben:

- Der Dateicode besitzt Ähnlichkeit mit einer bekannten Bedrohung, wurde aber teilweise verändert, oder er erinnert an die Struktur eines Schadprogramms, ist aber nicht in den Datenbanken enthalten. In diesem Fall wird die Datei aufgrund einer heuristischen Analyse, die von Datei-Anti-Virus oder Mail-Anti-Virus ausgeführt wird oder bei einer Virensuche erfolgt, in die Quarantäne verschoben. Der heuristische Analysemechanismus führt nur selten zu einem Fehlalarm.
- Die Aktionsfolge, die von einem Objekt ausgeführt werden soll, gilt als verdächtig. In diesem Fall wird die Datei aufgrund einer Verhaltensanalyse, die vom Proaktiven Schutz ausgeführt wird, in die Quarantäne verschoben.

Dateien, die unter Quarantäne stehen, stellen keine Gefahr dar. Im Lauf der Zeit erscheinen Informationen über neue Bedrohungen und entsprechende Desinfektionsmethoden. Dadurch kann sich die Möglichkeit ergeben, dass eine unter Quarantäne stehende Datei von Kaspersky Internet Security desinfiziert werden kann.

Backup dient zur Speicherung der Sicherungskopien von Dateien, die gelöscht oder bei der Desinfektion verändert wurden.

IN DIESEM ABSCHNITT

DATEIEN IN DER QUARANTÄNE UND IM BACKUP SPEICHERN

Die maximale Speicherdauer für Objekte beträgt standardmäßig 30 Tage. Danach werden die Objekte gelöscht. Sie können diese Zeitbeschränkung aufheben oder die maximale Speicherdauer für Objekte ändern.

Außerdem können Sie eine maximale Größe für die Quarantäne und das Backup festlegen. Beim Erreichen der maximalen Größe wird der Inhalt der Quarantäne und des Backups durch neue Objekte ersetzt. Die Größenbeschränkung ist standardmäßig deaktiviert.

➡ *Gehen Sie folgendermaßen vor, um eine maximale Speicherdauer für Objekte festzulegen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Quarantäne- und Backup-Objekte speichern** das Kontrollkästchen **Objekte speichern für maximal** und legen Sie eine maximale Speicherdauer für Quarantäneobjekte fest.

➡ *Gehen Sie folgendermaßen vor, um die maximale Größe für die Quarantäne und das Backup anzupassen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Quarantäne- und Backup-Objekte speichern** das Kontrollkästchen **Maximale Größe** und legen Sie eine maximale Größe für die Quarantäne und das Backup fest.

ARBEIT MIT DATEIEN IN DER QUARANTÄNE

Die Quarantäne von Kaspersky Internet Security ermöglicht die Ausführung folgender Operationen:

- Dateien, die Sie für infiziert halten, in die Quarantäne verschieben.
- Quarantänedateien mit den Datenbanken der aktuellen Version von Kaspersky Internet Security untersuchen.
- Dateien in den Ordnern wiederherstellen, aus denen sie in die Quarantäne verschoben wurden.
- Ausgewählte Dateien aus der Quarantäne entfernen.
- Quarantänedateien zur Untersuchung an Kaspersky Lab schicken.

Eine Datei kann auf folgende Arten in die Quarantäne verschoben werden:

- mit Hilfe der Schaltfläche **In die Quarantäne verschieben** im Fenster **Quarantäne**
- mit Hilfe des Kontextmenüs für die Datei.

➡ *Um eine Datei aus dem Fenster Quarantäne in die Quarantäne zu verschieben, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Quarantäne**.
3. Klicken Sie auf der Registerkarte **Quarantäne** auf die Schaltfläche **In die Quarantäne verschieben**.
4. Wählen Sie im folgenden Fenster die Datei, die in die Quarantäne verschoben werden soll.

➡ *Gehen Sie folgendermaßen vor, um eine Datei mit Hilfe des Kontextmenüs in die Quarantäne zu verschieben:*

1. Öffnen Sie das Fenster von Microsoft Windows Explorer und gehen Sie in den Ordner mit der Datei, die in die Quarantäne verschoben werden soll.
2. Öffnen Sie durch Rechtsklick das Kontextmenü für die Datei und wählen Sie den Punkt **In die Quarantäne verschieben**.

➡ *Um eine Quarantänedatei zu untersuchen, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Quarantäne**.
3. Wählen Sie auf der Registerkarte **Quarantäne** die Datei aus, die untersucht werden soll.
4. Klicken Sie auf die Schaltfläche **Prüfen**.

➡ *Gehen Sie folgendermaßen vor, um eine Datei aus der Quarantäne wiederherzustellen:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Quarantäne**.
3. Wählen Sie auf der Registerkarte **Quarantäne** die Datei aus, die wiederhergestellt werden soll.
4. Klicken Sie anschließend auf die Schaltfläche **Wiederherstellen**.

➡ *Gehen Sie folgendermaßen vor, um eine Datei aus der Quarantäne zu löschen:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Quarantäne**.
3. Wählen Sie auf der Registerkarte **Quarantäne** die Datei aus, die gelöscht werden soll.
4. Öffnen Sie durch Rechtsklick das Kontextmenü für die Datei und wählen Sie den Punkt **Löschen**.

➡ *Um ein Quarantäneobjekt zur Untersuchung an Kaspersky Lab zu schicken, gehen Sie wie folgt vor.*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Fensterbereich den Abschnitt **Quarantäne**.
3. Wählen Sie auf der Registerkarte **Quarantäne** die Datei aus, die zur Untersuchung geschickt werden soll.
4. Öffnen Sie durch Rechtsklick das Kontextmenü für eine Datei und wählen Sie den Punkt **Zur Analyse einsenden**.

ARBEIT MIT BACKUP-OBJEKTEN

Das Backup von Kaspersky Internet Security ermöglicht die Ausführung folgender Operationen:

- Dateien im vorgegebenen Ordner oder in den Ordnern wiederherstellen, in denen die Dateien vor der Verarbeitung durch Kaspersky Internet Security gespeichert wurden.
- Ausgewählte Dateien oder alle Dateien im Backup löschen.

➡ *Gehen Sie folgendermaßen vor, um eine Datei aus dem Backup wiederherzustellen:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie im unteren Fensterbereich den Abschnitt **Quarantäne**.

3. Wählen Sie auf der Registerkarte **Backup** die Datei aus, die wiederhergestellt werden soll.

4. Klicken Sie anschließend auf die Schaltfläche **Wiederherstellen**.

➡ *Gehen Sie folgendermaßen vor, um eine Datei aus dem Backup zu löschen:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie im unteren Fensterbereich den Abschnitt **Quarantäne**.

3. Wählen Sie auf der Registerkarte **Backup** die Datei aus, die gelöscht werden soll.

4. Öffnen Sie durch Rechtsklick das Kontextmenü für die Datei und wählen Sie den Punkt **Löschen**.

➡ *Gehen Sie folgendermaßen vor, um alle Dateien aus dem Backup zu löschen:*

1. Öffnen Sie das Programmhauptfenster.

2. Wählen Sie im unteren Fensterbereich den Abschnitt **Quarantäne**.

3. Klicken Sie auf der Registerkarte **Backup** auf die Schaltfläche **Speicher leeren**.

QUARANTÄNEDATEIEN NACH DEM UPDATE UNTERSUCHEN

Wenn sich bei der Untersuchung nicht genau ermitteln lässt, von welchen Schadprogrammen eine Datei infiziert ist, wird die Datei in die Quarantäne verschoben. Möglicherweise kann die Bedrohung eindeutig bestimmt und desinfiziert werden, nachdem die Datenbanken von Kaspersky Internet Security aktualisiert wurden. Sie können eine automatische Untersuchung der Quarantänedateien nach jedem Update festlegen.

Es wird empfohlen, die Dateien in der Quarantäne regelmäßig zu überprüfen. Aufgrund der Untersuchung kann sich ihr Status ändern. Bestimmte Dateien können am ursprünglichen Ort wiederhergestellt und wiederverwendet werden.

➡ *Gehen Sie folgendermaßen vor, um festzulegen, dass die Quarantänedateien nach einem Update automatisch untersucht werden:*

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Update** die Komponente **Update-Einstellungen**.

3. Aktivieren Sie im Block **Erweitert** das Kontrollkästchen **Quarantänedateien nach jedem Update untersuchen**.

ZUSÄTZLICHE SCHUTZ-TOOLS

Zum Lieferumfang von Kaspersky Internet Security gehören verschiedene Assistenten und Tools, mit denen Aufgaben für die Computersicherheit gelöst werden.

- Der Notfall-CD-Assistent dient dazu, ein Abbild zu erstellen und das Notfall-CD-Programm auf einen Wechseldatenträger zu schreiben. Das Notfall-CD-Programm ermöglicht die Wiederherstellung des Systems nach einem Virenangriff durch das Booten von einem Wechseldatenträger. Das Notfall-CD-Programm kommt dann zum Einsatz, wenn der Infektionsgrad so hoch ist, dass die Desinfektion eines Computers nicht mehr mit Hilfe von Anti-Viren-Anwendungen oder Desinfektions-Tools möglich ist.

- Der Lösch-Assistent für Aktivitätsspuren dient dazu, im System nach Aktivitätsspuren eines Benutzers sowie auch nach Betriebssystemparametern, die zum Sammeln von Informationen über die Aktivität des Benutzers dienen, zu suchen und diese zu beseitigen.

- Der Systemwiederherstellungs-Assistent dient dazu, Beschädigungen des Systems und die Spuren von schädlichen Objekten im System zu beseitigen.
- Der Browser-Konfigurations-Assistent dient dazu, die Einstellungen des Browsers Microsoft Internet Explorer zu analysieren und anzupassen, um potenzielle Schwachstellen zu beseitigen.

Alle Probleme, die von den Assistenten gefunden werden (unter Ausnahme des Notfall-CD-Assistenten) werden im Hinblick auf die von ihnen für das System ausgehende Gefahr eingeteilt. Für jede Gruppe von Problemen schlagen die Kaspersky-Lab-Spezialisten eine Auswahl von Aktionen vor, mit denen die Schwachstellen und kritischen Punkte im System behoben werden können. Die Probleme und die entsprechenden Aktionen werden in drei Gruppen unterteilt:

- *Ausdrücklich empfohlene Aktionen* können Probleme beheben, die eine ernsthafte Sicherheitsbedrohung darstellen. Es wird empfohlen, alle Aktionen dieser Gruppe rechtzeitig auszuführen, um die Bedrohungen zu beseitigen.
- *Empfohlene Aktionen* dienen zum Beheben von Problemen, die ein potenzielles Risiko darstellen können. Um einen optimalen Schutz zu gewährleisten, sollten auch die Aktionen dieser Gruppe ausgeführt werden.
- *Zusätzliche Aktionen* dienen dazu, momentan ungefährliche Probleme zu beheben, die die Computersicherheit jedoch in Zukunft bedrohen können. Diese Vorgehensweise sorgt für einen vollständigen Schutz Ihres Computers, kann aber in einigen Fällen zu einem Löschen von Benutzereinstellungen (z.B. von Cookies) führen.

IN DIESEM ABSCHNITT

AKTIVITÄTSSPUREN LÖSCHEN

Während der Arbeit auf dem Computer werden die Aktionen des Benutzers im System registriert. Dabei werden Daten darüber gespeichert, welche Suchanfragen der Benutzer vornimmt, welche Seiten er besucht, welche Programme er startet und welche Dateien er öffnet und speichert. Außerdem werden Einträge im Systemjournal von Microsoft Windows, temporäre Dateien u.v.a gespeichert.

Alle genannten Informationsquellen über die Benutzeraktivität können sensible Daten (darunter auch Kennwörter) enthalten und können unter Umständen von Angreifern entwendet und analysiert werden. Viele Benutzer verfügen nicht über ausreichende Kenntnisse, um einem Diebstahl wertvoller Informationen aus solchen Quellen vorzubeugen.

Kaspersky Internet Security verfügt über einen Lösch-Assistenten für Aktivitätsspuren. Dieser Assistent führt im System die Suche nach Spuren von Benutzeraktivität und den Betriebssystemparametern, die zum Sammeln von Informationen über die Aktivität dienen, durch.

Es sollte beachtet werden, dass laufend Informationen über die Aktivität des Benutzers im System gesammelt werden. Der Start einer beliebigen Datei oder das Öffnen eines Dokuments werden in einem Verlauf festgehalten, und das Systemjournal von Microsoft Windows registriert eine Vielzahl von Ereignissen, die im System vorfallen. Deshalb kann es sein, dass bei einem wiederholten Start des Lösch-Assistenten für Aktivitätsspuren gefunden werden, die beim vorhergehenden Start des Assistenten bereits gelöscht worden sind. Es kann vorkommen, dass bestimmte Dateien, wie z.B. eine Journaldatei von Microsoft Windows, vom System verwendet werden, während sie vom Assistenten gelöscht werden sollen. Um diese Dateien zu löschen, schlägt der Assistent vor, das System neu zu starten. Im Verlauf eines Neustarts können solche Dateien aber erneut erstellt werden, was dazu führt, dass sie wieder als Aktivitätsspuren erkannt werden.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

➡ *Gehen Sie folgendermaßen vor, um die Aktivitätsspuren eines Benutzers im System zu löschen:*

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Bereich des Fensters den Abschnitt **Tools**.
3. Klicken Sie im folgenden Fenster im Block **Löschen von Aktivitätsspuren** auf die Schaltfläche **Ausführen**.

Details zu den einzelnen Schritten des Assistenten

Schritt 1. Assistent starten

Vergewissern Sie sich, dass die Variante **Diagnose der Spuren von Benutzeraktivität durchführen** gewählt wurde, und klicken Sie auf **Weiter**, um den Assistenten zu starten.

Schritt 2. Suche von Aktivitätsspuren

Der Assistent führt auf Ihrem Computer die Suche nach Aktivitätsspuren aus. Die Suche kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für das Löschen von Aktivitätsspuren wählen

Nach dem Abschluss der Suche informiert der Assistent über die gefundenen Aktivitätsspuren und mögliche Aktionen, um sie zu beseitigen.

Klicken Sie links vom Namen einer Gruppe auf das Zeichen **+**, um die Aktionen der Gruppe anzuzeigen.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen.

> Die standardmäßig aktivierten Kontrollkästchen sollten auf keinen Fall entfernt werden, da hierdurch die Sicherheit Ihres Computers bedroht wird.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Aktivitätsspuren löschen

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Das Löschen von Aktivitätsspuren kann eine gewisse Zeit beanspruchen. Um bestimmte Aktivitätsspuren zu löschen, kann ein Neustart des Computers erforderlich sein. Darüber werden Sie vom Assistenten informiert.

Nach Abschluss des Vorgangs wechselt der Assistent automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Damit das Löschen von Aktivitätsspuren in Zukunft automatisch erfolgt, wenn Kaspersky Internet Security beendet wird, aktivieren Sie beim letzten Schritt des Assistenten das Kontrollkästchen **Löschen von Aktivitätsspuren jedes Mal beim Beenden von Kaspersky Internet Security ausführen**. Wenn Sie planen, die Aktivitätspuren künftig selbst zu beseitigen, lassen Sie dieses Kontrollkästchen deaktiviert.

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

BROWSER-SICHERHEITSEINSTELLUNGEN KONFIGURIEREN

In bestimmten Fällen ist es notwendig, den Browser Microsoft Internet Explorer auf spezielle Weise zu analysieren und anzupassen, da benutzerdefinierte oder standardmäßige Einstellungen zu Sicherheitsproblemen führen können.

Beispiele für Objekte und Einstellungen, die vom Browser verwendet werden und potenzielle Sicherheitsrisiken bergen:

- **Zwischenspeicher für die Arbeit von Microsoft Internet Explorer**. Im Cache werden Daten gespeichert, die aus dem Internet heruntergeladen wurden. So lässt sich ein erneuter Download vermeiden. Dadurch wird die Ladedauer für Webseiten reduziert und der Internet-Datenverkehr verringert. Allerdings enthält der Zwischenspeicher vertrauliche Daten und kann außerdem Aufschluss darüber geben, welche Ressourcen ein Benutzer besucht hat. Viele schädliche Objekte lesen beim Scannen der Festplatte auch den Zwischenspeicher. Auf diese Weise können Angreifer beispielsweise die Mail-Adressen von Benutzern erhalten. Zur Optimierung des Schutzes wird empfohlen, den Zwischenspeicher zu leeren, wenn die Arbeit mit dem Browser beendet wird.

- **Anzeige von Erweiterungen für dem System bekannte Dateitypen**. Um das Umbenennen von Dateien zu erleichtern, können die Erweiterungen ausgeblendet werden. Allerdings ist es für den Benutzer manchmal besser, die tatsächliche Dateierweiterung zu sehen. Häufig werden in den Namen schädlicher Objekte Zeichenfolgen verwendet, in denen der echten Erweiterung zu Imitationszwecken eine zusätzliche Erweiterung vorangestellt wird (z.B. example.txt.com). Wenn die tatsächliche Dateierweiterung nicht angezeigt wird, sieht der Benutzer nur den Teil des Dateinamens, der die imitierte Erweiterung enthält, und kann das schädliche Objekt für eine unschädliche Datei halten. Zur Optimierung des Schutzes wird empfohlen, die Anzeige von Erweiterungen für Dateien bekannter Formate zu aktivieren.

- **Liste mit vertrauenswürdigen Seiten**. Um problemlos mit bestimmten Webseiten arbeiten zu können, müssen sie der vertrauenswürdigen Liste hinzugefügt werden. Allerdings können schädliche Objekte einer solchen Liste Links zu Webseiten hinzufügen, die von Angreifern erstellt wurden.

Sicherheitsbezogene Browser-Einstellungen können bei der Anzeige bestimmter Webseiten zu Problemen führen (beispielsweise auf Webseiten, die ActiveX-Elemente einsetzen). Das Problem lässt sich lösen, indem solche Webseiten in die vertrauenswürdige Zone aufgenommen werden.

Die Analyse und Konfiguration des Browsers wird vom Browser-Konfigurations-Assistenten ausgeführt. Der Assistent prüft, ob die aktuellen Updates für den Browser installiert sind und ob die Browser-Einstellungen keine Schwachstellen aufweisen, die das System verletzbar machen. Beim Abschluss des Assistenten wird ein Bericht erstellt, der zur Analyse an Kaspersky Lab geschickt werden kann.

Der Assistent besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Zurück** und **Weiter**. Zum Abschluss des Assistenten dient die Schaltfläche **Beenden**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf **Abbrechen** abgebrochen werden.

Schließen Sie alle Browserfenster von Microsoft Internet Explorer, bevor mit der Diagnose begonnen wird.

Gehen Sie folgendermaßen vor, um die Sicherheitseinstellungen des Browsers zu konfigurieren:

1. Öffnen Sie das Programmhauptfenster.
2. Wählen Sie im unteren Bereich des Fensters den Abschnitt **Tools**.
3. Klicken Sie im folgenden Fenster im Block **Browser-Konfiguration** auf die Schaltfläche **Ausführen**.

Details zu den einzelnen Schritten des Assistenten

Schritt 1. Assistent starten

Vergewissern Sie sich, dass die Variante **Diagnose von Microsoft Internet Explorer durchführen** gewählt wurde, und klicken Sie auf **Weiter**, um den Assistenten zu starten.

Schritt 2. Analyse der Einstellungen von Microsoft Internet Explorer

Der Assistent analysiert die Einstellungen des Browsers Microsoft Internet Explorer. Die Suche nach Problemen in den Einstellungen des Browsers kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Aktionen für die Browser-Konfiguration wählen

Nach Abschluss der Suche informiert der Assistent über die gefundenen Probleme und schlägt Aktionen zu deren Beseitigung vor.

Klicken Sie links vom Namen einer Gruppe auf das Zeichen **+**, um die Aktionen der Gruppe anzuzeigen.

Um eine bestimmte Aktion auszuführen, aktivieren Sie das Kontrollkästchen links vom Namen der Aktion. In der Grundeinstellung werden alle empfohlenen und ausdrücklich empfohlenen Aktionen ausgeführt. Soll eine bestimmte Aktion nicht ausgeführt werden, dann deaktivieren Sie das entsprechende Kontrollkästchen.

Die standardmäßig aktivierten Kontrollkästchen sollten auf keinen Fall entfernt werden, da hierdurch die Sicherheit Ihres Computers bedroht wird.

Klicken Sie auf **Weiter**, nachdem Sie die Aktionen gewählt haben, die der Assistent ausführen soll.

Schritt 4. Browser-Konfiguration

Der Assistent führt die Aktionen aus, die beim vorherigen Schritt festgelegt wurden. Die Browser-Konfiguration kann eine gewisse Zeit beanspruchen. Der Assistent geht nach Abschluss der Konfiguration automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

ÄNDERUNGEN RÜCKGÄNGIG MACHEN, DIE VON DEN ASSISTENTEN AUSGEFÜHRT WURDEN

Bestimmte Änderungen, die beim Start des Assistenten zum Löschen von Aktivitätsspuren (s. Abschnitt "Aktivitätsspuren löschen" auf S. 173), des Assistenten zur Systemwiederherstellung (s. Abschnitt "Was tun, wenn Sie vermuten, dass Ihr Computer infiziert ist?" auf S. 56) und des Assistenten zur Browser-Konfiguration (s. Abschnitt "Browser-Sicherheitseinstellungen konfigurieren" auf S. 174) ausgeführt wurden, können rückgängig gemacht werden.

Gehen Sie folgendermaßen vor, um die von den Assistenten vorgenommenen Änderungen rückgängig zu machen:

1. Öffnen Sie das Programmhauptfenster und wählen Sie unten im Fenster den Abschnitt **Tools**.
2. Klicken Sie im rechten Fensterbereich im Block mit dem Namen des Assistenten, für welchen die vorgenommenen Änderungen rückgängig gemacht werden sollen, auf die Schaltfläche **Ausführen**:
   - **Löschen von Aktivitätsspuren**, um die vom Lösch-Assistenten für Aktivitätsspuren vorgenommenen Änderungen rückgängig zu machen.
   - **Wiederherstellung nach Infektion**, um die vom Systemwiederherstellungs-Assistenten vorgenommenen Änderungen rückgängig zu machen.
   - **Browser-Konfiguration**, um die vom Browser-Konfigurationsassistenten vorgenommenen Änderungen rückgängig zu machen.

Im Folgenden wird beschrieben, welche Schritte der Assistent bei einem Rollback von Änderungen ausführt.

Schritt 1. Assistent starten

Wählen Sie die Variante **Änderungen verwerfen** und klicken Sie auf **Weiter**.

Schritt 2. Änderungen suchen

Der Assistent sucht nach Veränderungen, die er früher ausgeführt hat und für die ein Rollback möglich ist. Der Assistent geht nach Abschluss der Suche automatisch zum nächsten Schritt.

Schritt 3. Veränderungen wählen, die zurückgenommen werden sollen.

Nach Abschluss der Suche benachrichtigt der Assistent über erkannte Änderungen.

Damit der Assistent eine früher ausgeführte Aktion abbricht, aktivieren Sie das Kontrollkästchen für die entsprechende Aktion.

Nachdem Sie Aktionen ausgewählt haben, die abgebrochen werden sollen, klicken Sie auf die Schaltfläche **Weiter**.

Schritt 4. Änderungen rückgängig machen

Der Assistent bricht die Aktionen ab, die im vorherigen Schritt ausgewählt wurden. Anschließend wechselt der Assistent automatisch zum nächsten Schritt.

Schritt 5. Assistent abschließen

Klicken Sie auf **Beenden**, um den Assistenten abzuschließen.

BERICHTE

Die Ereignisse, die während der Arbeit der Schutzkomponenten oder bei der Ausführung von Aufgaben von Kaspersky Internet Security eintreten, werden in Berichten festgehalten.

IN DIESEM ABSCHNITT

BERICHT FÜR EINE BESTIMMTE SCHUTZKOMPONENTE ERSTELLEN

Sie können einen detaillierten Bericht über die Ereignisse erhalten, die bei der Ausführung der einzelnen Schutzkomponenten und Aufgaben von Kaspersky Internet Security eintreten.

Zur übersichtlichen Arbeit mit Berichten können Sie die Darstellung von Daten auf dem Bildschirm ändern: Ereignisse nach unterschiedlichen Parametern anordnen, Berichtszeitraum wählen, Ereignisse nach einer Spalte oder nach Priorität anordnen, Tabellenspalten ausblenden.

Gehen Sie folgendermaßen vor, um einen Bericht für eine Schutzkomponente oder Aufgabe zu erhalten:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Fensterbereich auf den Link **Berichte**.
3. Klicken Sie im folgenden Fenster **Berichte** auf die Schaltfläche **Detaillierter Bericht**.
4. Wählen Sie im folgenden Fenster **Detaillierter Bericht** links eine Komponente oder Aufgabe, für die ein Bericht erstellt werden soll. Bei Auswahl des Punkts **Schutz-Center** wird ein Bericht für alle Schutzkomponenten erstellt.

DATENFILTERUNG

Die Ereignisse in den Berichten für Kaspersky Internet Security können nach einem oder mehreren Werten in den Tabellenspalten gefiltert werden. Außerdem lassen sich komplexe Bedingungen für die Datenfilterung festlegen.

Gehen Sie folgendermaßen vor, um die Ereignisse nach Werten zu filtern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Fensterbereich auf den Link **Berichte**.
3. Klicken Sie im folgenden Fenster **Berichte** auf die Schaltfläche **Detaillierter Bericht**.
4. Zeigen Sie auf der rechten Seite des folgenden Fensters **Detaillierter Bericht** mit der Maus auf die linke obere Ecke der Überschrift einer Tabellenspalte und öffnen Sie durch Linksklick das Filtermenü.
5. Wählen Sie im Filtermenü den Wert, nach dem die Daten gefiltert werden sollen.
6. Wiederholen Sie den Vorgang bei Bedarf für eine andere Tabellenspalte.

Gehen Sie folgendermaßen vor, um eine komplexe Filterbedingung festzulegen:

1. Öffnen Sie das Programmhauptfenster.
2. Öffnen Sie mit dem Link **Berichte** im oberen Fensterbereich das Fenster für Berichte.
3. Klicken Sie im folgenden Fenster auf der Registerkarte **Bericht** auf die Schaltfläche **Detaillierter Bericht**.
4. Öffnen Sie auf der rechten Seite des folgenden Fensters **Detaillierter Bericht** durch Rechtsklick das Kontextmenü für die entsprechende Berichtspalte und wählen Sie dort den Punkt **Filter**.
5. Legen Sie im folgenden Fenster **Benutzerdefinierter Filter** die Filterbedingungen fest.
    a. Legen Sie auf der rechten Fensterseite die Auswahlgrenzen fest.
    b. Wählen Sie auf der linken Fensterseite in der Dropdown-Liste **Bedingung** eine Auswahlbedingung fest (z.B.: größer oder kleiner, gleich oder ungleich mit dem Wert, der als Auswahlgrenze angegeben wurde).
    c. Fügen Sie bei Bedarf eine zweite Bedingung hinzu. Verwenden Sie dazu die logischen Operationen Konjunktion (logisches UND) und Disjunktion (logisches ODER). Wenn Sie möchten, dass der Datenzugriff beide festgelegte Bedingungen erfüllt, wählen Sie **UND** aus. Ist eine Bedienung ausreichend, dann wählen Sie **ODER** aus.

SUCHE NACH EREIGNISSEN

Um in einem Bericht nach einem bestimmten Ereignis zu suchen, können Sie entweder in der Suchzeile oder in einem speziellen Fenster ein Schlüsselwort eingeben.

Gehen Sie folgendermaßen vor, um mit der Suchzeile nach einem Ereignis zu suchen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Fensterbereich auf den Link **Berichte**.
3. Klicken Sie im folgenden Fenster **Berichte** auf die Schaltfläche **Detaillierter Bericht**.
4. Geben Sie auf der rechten Seite des folgenden Fensters **Detaillierter Bericht** in der Suchzeile ein Schlüsselwort ein.

Gehen Sie folgendermaßen vor, um mit dem Suchfenster nach einem Ereignis zu suchen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Fensterbereich auf den Link **Berichte**.
3. Klicken Sie im folgenden Fenster **Berichte** auf die Schaltfläche **Detaillierter Bericht**.
4. Öffnen Sie auf der rechten Seite des folgenden Fensters **Detaillierter Bericht** durch Rechtsklick das Kontextmenü für die Überschrift der entsprechenden Spalte und wählen Sie dort den Punkt **Suche**.
5. Legen Sie im folgenden **Fenster** Suche die Suchkriterien fest.
   a. Geben Sie im Feld **Zeile** das gesuchte Schlüsselwort ein.
   b. Wählen Sie in der Dropdown-Liste **Spalte** den Namen der Spalte, in der nach dem angegebenen Schlüsselwort gesucht werden soll.
   c. Aktivieren Sie bei Bedarf die Kontrollkästchen für zusätzliche Sucheinstellungen.
6. Starten Sie die Suche auf folgende Weise:
   - Wenn Sie nach dem nächsten markierten Ereignis in der Liste suchen möchten, das die vorgegebenen Suchkriterien erfüllt, klicken Sie auf die Schaltfläche **Weitersuchen**.
   - Wenn Sie alle Ereignisse finden möchten, welche die vorgegebenen Suchkriterien erfüllen, klicken Sie auf die Schaltfläche **Alle markieren**.

BERICHT IN DATEI SPEICHERN

Der Bericht kann in einer Textdatei gespeichert werden.

Gehen Sie folgendermaßen vor, um den Bericht in einer Datei zu speichern:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Fensterbereich auf den Link **Berichte**.
3. Klicken Sie im folgenden Fenster **Berichte** auf die Schaltfläche **Detaillierter Bericht**.
4. Erstellen Sie im folgenden Fenster **Detaillierter Bericht** den gewünschten Bericht, und öffnen Sie durch Klicken auf den Link **Speichern** das Fenster zur Auswahl des Ortes für die zu speichernde Datei.
5. Geben Sie im folgenden Fenster den Ordner an, in dem die Berichtsdatei gespeichert werden soll, und nennen Sie einen Dateinamen.

BERICHTE SPEICHERN

Die standardmäßige Speicherdauer für Ereignisberichte beträgt 30 Tage. Danach werden die Daten gelöscht. Sie können diese Zeitbeschränkung aufheben oder die maximale Speicherdauer für Berichte ändern.

Außerdem können Sie eine maximale Größe für eine Berichtsdatei festlegen. Die maximale Größe beträgt standardmäßig 1024 MB. Beim Erreichen der maximalen Größe wird der Inhalt der Datei durch neue Einträge ersetzt. Sie können die Größenbeschränkung aufheben oder einen anderen Wert festlegen.

➡ *Gehen Sie folgendermaßen vor, um eine maximale Speicherdauer für Ereignisberichte festzulegen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Berichte speichern** das Kontrollkästchen **Berichte speichern für maximal** und legen Sie eine maximale Speicherdauer für Berichte fest.

➡ *Gehen Sie folgendermaßen vor, um die maximale Größe einer Berichtsdatei festzulegen:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.
3. Aktivieren Sie auf der rechten Fensterseite im Block **Berichte speichern** das Kontrollkästchen **Maximale Dateigröße** und legen Sie die maximale Größe einer Berichtsdatei fest.

BERICHTE LEEREN

Berichte, deren Daten Sie nicht mehr benötigen, können bereinigt werden.

➡ *Um die* Berichte zu leeren*, gehen Sie folgendermaßen vor*:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.
3. Klicken Sie auf der rechten Fensterseite im Block **Berichte leeren** auf **Leeren...**.
4. Aktivieren Sie im folgenden Fenster **Berichte löschen** die Kontrollkästchen der Berichte, die Sie bereinigen möchten.

NICHT KRITISCHE EREIGNISSE PROTOKOLLIEREN

Einträge über nicht kritische Ereignisse sowie Ereignisse, welche die Registrierung und das Dateisystem betreffen, werden in der Grundeinstellung nicht protokolliert. Sie können die Protokollierung solcher Einträge aktivieren.

➡ *Damit nicht kritische Ereignisse protokolliert werden, gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Berichte und Speicher**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Protokollierung von nicht kritischen Ereignissen aktivieren**.

BENACHRICHTIGUNG ÜBER DIE BEREITSCHAFT EINES BERICHTS ANPASSEN

Sie können einen Zeitplan erstellen, nach dem Kaspersky Internet Security Sie über die Bereitschaft eines Berichts benachrichtigen soll.

Um die Benachrichtigung über die Bereitschaft eines Berichts anzupassen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Fensterbereich auf den Link **Berichte**.
3. Klicken Sie im folgenden Fenster **Berichte** auf die Schaltfläche .
4. Legen Sie im folgenden Fenster **Meldungen** die Zeitplan-Einstellungen fest.

AUSSEHEN DES PROGRAMMS. AKTIVE ELEMENTE DER BENUTZEROBERFLÄCHE VERWALTEN

In Kaspersky Internet Security können Sie Einstellungen für die Textanzeige auf dem Windows-Begrüßungsbildschirm sowie Einstellungen für die aktiven Elemente der Benutzeroberfläche (Programmsymbol im Infobereich, Meldungsfenster und Pop-up-Meldungen) konfigurieren.

IN DIESEM ABSCHNITT

HALBTRANSPARENZ FÜR MELDUNGSFENSTER

Gehen Sie folgendermaßen vor, um die Halbtransparenz der Meldungsfenster zu aktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Ansicht**.
3. Aktivieren Sie im Block **Symbol in der Taskleiste** das Kontrollkästchen **Transparenz für Meldungsfenster verwenden**.

ANIMATION DES PROGRAMMSYMBOLS IM INFOBEREICH

Die Animation des Programmsymbols wird im Infobereich angezeigt, wenn das Update oder eine Untersuchung ausgeführt wird.

Standardmäßig ist die Animation des Programmsymbols im Infobereich aktiviert.

Gehen Sie folgendermaßen vor, um die Animation des Programmsymbols zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Ansicht**.
3. Deaktivieren Sie im Block **Symbol in der Taskleiste** das Kontrollkästchen **Animation des Symbols bei Aufgabenausführung verwenden**.

TEXT AUF DEM WINDOWS-BEGRÜßUNGSBILDSCHIRM

Wenn Kaspersky Internet Security aktiviert ist und der Schutz Ihres Computers funktioniert, wird beim Starten von Windows auf dem Begrüßungsbildschirm die Zeile "Protected by Kaspersky Lab" angezeigt.

Der Text "Protected by Kaspersky Lab" wird nur unter Microsoft Windows XP angezeigt.

Gehen Sie folgendermaßen vor, um die Textanzeige beim Starten von Windows zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Ansicht**.
3. Deaktivieren Sie im Block **Symbol in der Taskleiste** das Kontrollkästchen **"Protected by Kaspersky Lab" über dem Microsoft Windows-Begrüßungsbildschirm anzeigen**.

MELDUNGEN

Standardmäßig werden Sie beim Auftreten von Ereignissen während der Ausführung von Kaspersky Internet Security entsprechend informiert. Wenn Sie über das weitere Vorgehen entscheiden sollen, erscheinen auf dem Bildschirm Meldungsfenster (s. Abschnitt "Meldungsfenster und Pop-up-Meldungen" auf S. 36). Über Ereignisse, die keine Auswahl des weiteren Vorgehens erfordern, informiert das Programm mit Hilfe von akustischen Signalen, E-Mails und Pop-up-Meldungen im Infobereich der Taskleiste (s. Abschnitt "Meldungsfenster und Pop-up-Meldungen" auf S. 36).

Zu Kaspersky Internet Security gehört ein News Agent (auf S. 40), über den Sie von Kaspersky Lab benachrichtigt werden. Wenn Sie keine Nachrichten empfangen möchten, können Sie den Empfang von Nachrichten deaktivieren.

IN DIESEM ABSCHNITT

MELDUNGEN AKTIVIEREN UND DEAKTIVIEREN

Standardmäßig benachrichtigt Sie Kaspersky Internet Security auf verschiedene Arten über wichtige Ereignisse im Zusammenhang mit der Ausführung des Programms (s. Abschnitt "Benachrichtigungsmethode anpassen" auf S. 183). Sie können das Senden von Benachrichtigungen deaktivieren.

Die Informationen über Ereignisse, die während der Ausführung von Kaspersky Internet Security auftreten, werden unabhängig davon, ob die Benachrichtigungen aktiviert oder deaktiviert sind, im Bericht über die Programmaktivität protokolliert (s. S. 177).

Die Deaktivierung der Benachrichtigungen beeinflusst die Anzeige der Meldungsfenster nicht. Um nur eine minimale Anzahl an Meldungsfenstern auf dem Bildschirm anzeigen zu lassen, verwenden Sie den automatischen Schutzmodus (s. Abschnitt "Schutzmodus auswählen" auf S. 68).

Gehen Sie folgendermaßen vor, um das Senden von Meldungen zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Meldungen**.
3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Ereignisse melden**.

BENACHRICHTIGUNGSMETHODE ANPASSEN

Das Programm informiert Sie auf folgende Arten über Ereignisse:

- durch Pop-up-Meldungen im Infobereich der Taskleiste;
- durch ein akustisches Signal;
- per E-Mail.

Sie können die Benachrichtigungsmethoden für jede Art von Ereignis individuell einstellen.

Kritische Meldungen und Meldungen über Störungen des Programms werden standardmäßig von akustischen Signalen begleitet. Für die Audiosignale wird das Soundschema Microsoft Windows verwendet. Sie können ein anderes Schema wählen oder die Tonsignale ausschalten.

Damit Kaspersky Internet Security Sie per E-Mail über Ereignisse benachrichtigen kann, müssen Sie die entsprechenden Einstellungen für die Zustellung per E-Mail vornehmen.

Gehen Sie folgendermaßen vor, um die Benachrichtigungsmethoden für verschiedene Ereignistypen auszuwählen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Meldungen**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Ereignisse melden** und klicken Sie auf die unterhalb des Kontrollkästchens angeordnete Schaltfläche **Einstellungen**.
4. Aktivieren Sie im erscheinenden Fenster **Meldungen** die Kontrollkästchen je nachdem, wie Sie Ihre Benachrichtigungen über die verschiedenen Ereignisse erhalten möchten: per E-Mail, in Form von Pop-up-Meldungen oder per akustischem Signal.

Gehen Sie folgendermaßen vor, um die E-Mail-Einstellungen für das Senden von Meldungen anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Meldungen**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **E-Mails über Ereignisse senden** und klicken Sie auf **Einstellungen**.
4. Passen Sie im folgenden Fenster **E-Mail-Meldungen anpassen** die Einstellungen für das Senden von Benachrichtigungen per E-Mail an.

Gehen Sie folgendermaßen vor, um das Soundschema anzupassen:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Meldungen**.

3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Audiosignale für Meldungen aktivieren**.

   Wenn Sie für die Benachrichtigung über die Ereignisse von Kaspersky Internet Security das Microsoft Windows-Soundschema verwenden möchten, aktivieren Sie das Kontrollkästchen **Standard-Soundschema 'Windows Default' verwenden**. Wenn das Kontrollkästchen deaktiviert ist, wird für die Klänge das Soundschema der vorhergehenden Version von Kaspersky Internet Security verwendet.

EMPFANG VON NACHRICHTEN DEAKTIVIEREN

Gehen Sie folgendermaßen vor, um den Empfang von Nachrichten aus dem Programmkonfigurationsfenster zu deaktivieren:

1. Öffnen Sie das Programmkonfigurationsfenster.

2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Ansicht**.

3. Deaktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Über Neuigkeiten benachrichtigen**.

KASPERSKY SECURITY NETWORK

Um die Effektivität des Schutzes Ihres Computers zu erhöhen, verwendet Kaspersky Internet Security die von Benutzern aus der ganzen Welt empfangenen Daten. Zur Sammlung dieser Daten dient Kaspersky Security Network.

Kaspersky Security Network (KSN) ist eine Infrastruktur der Online-Dienste und -Services, die den Zugriff auf die aktuelle Wissensdatenbank von Kaspersky Lab über den "Ruf" der Dateien, Internet-Ressourcen und Programme bietet. Durch die Verwendung der Daten von Kaspersky Security Network wird die Geschwindigkeit der Reaktion von Kaspersky Internet Security auf neue Bedrohungen und die Leistungsfähigkeit einiger Komponenten erhöht. Außerdem wird dadurch das Risiko verringert, dass Fehlalarme auftreten.

Die Teilnahme von Benutzern am Kaspersky Security Network ermöglicht es, schnell Informationen über Typen und Quellen neuer Bedrohungen zu sammeln, Neutralisierungsmethoden zu entwickeln und die Anzahl an Fehlalarmen zu reduzieren.

Darüber hinaus erhalten Sie durch die Teilnahme am Kaspersky Security Network Zugriff auf die Reputations-Datenbanken für Programme und Webseiten.

Bei Teilnahme am Kaspersky Security Network wird eine bestimmte Statistik, die während der Ausführung von Kaspersky Internet Security auf Ihrem Computer erstellt wird, automatisch an Kaspersky Lab übermittelt.

Es werden keine persönlichen Daten gesammelt, verarbeitet oder gespeichert.

Die Teilnahme an Kaspersky Security Network ist freiwillig. In der Regel entscheiden Sie im Verlauf der Installation von Kaspersky Internet Security über die Teilnahme. Allerdings können Sie Ihre Entscheidung jederzeit ändern.

IN DIESEM ABSCHNITT

TEILNAHME AN KASPERSKY SECURITY NETWORK AKTIVIEREN UND DEAKTIVIEREN

➧ *Zur Teilnahme an Kaspersky Security Network gehen Sie folgendermaßen vor:*

1. Öffnen Sie das Programmkonfigurationsfenster.
2. Wählen Sie auf der linken Fensterseite im Abschnitt **Erweiterte Einstellungen** den Abschnitt **Feedback**.
3. Aktivieren Sie auf der rechten Fensterseite das Kontrollkästchen **Ich akzeptiere die Teilnahmebedingungen des Kaspersky Security Network**.

VERBINDUNG ZUM KASPERSKY SECURITY NETWORK PRÜFEN

Mögliche Gründe, warum keine Verbindung mit dem Kaspersky Security Network besteht:

- Ihr Computer ist mit dem Internet nicht verbunden.
- Sie nehmen an Kaspersky Security Network nicht teil.
- Ihre Lizenz von Kaspersky Internet Security ist abgelaufen.

➧ *Gehen Sie folgendermaßen vor, um zu prüfen, ob eine Verbindung zum Kaspersky Security Network besteht:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im oberen Fensterbereich auf **Cloud-Sicherheit**.
3. Im linken Bereich des folgenden Fensters wird der Status der Verbindung zum Kaspersky Security Network angezeigt.

ÜBERPRÜFUNG DER PROGRAMMFUNKTION

Dieser Abschnitt beschreibt, wie die Programmfunktion überprüft und sichergestellt wird, ob das Programm Viren und deren Modifikationen korrekt erkennt und entsprechend behandelt.

IN DIESEM ABSCHNITT

ÜBER DIE EICAR-TESTDATEI

Mit Hilfe der *EICAR-Testdatei* können Sie sich vergewissern, ob das Programm Viren korrekt erkennt und infizierte Dateien desinfiziert. Die EICAR-Testdatei wurde vom European Institute for Computer Antivirus Research (EICAR) entwickelt, um die Funktion von Antiviren-Programmen zu überprüfen.

Die EICAR-Testdatei ist kein Virus. Die EICAR-Testdatei enthält keinen Programmcode, der Ihren Computer beschädigen könnte. Trotzdem wird die EICAR-Testdatei von den meisten Antiviren-Programmen als Virus identifiziert.

Die EICAR-Testdatei eignet sich nicht zur Überprüfung der heuristischen Analyse und der Malware-Suche auf Systemebene (Rootkit-Suche).

Verwenden Sie nie echte Viren, um die Funktionsfähigkeit von Antiviren-Programmen zu testen! Dadurch könnte Ihr Computer ernsthaft beschädigt werden.

Denken Sie unbedingt daran, den Virenschutz für den Internet-Datenverkehr und den Virenschutz für Dateien wieder zu aktivieren, nachdem die Überprüfung mit der EICAR-Testdatei abgeschlossen wurde.

ÜBERPRÜFUNG DER PROGRAMMFUNKTION UNTER VERWENDUNG DER EICAR-TESTDATEI

Sie können mit der EICAR-Testdatei überprüfen, ob der Schutz für den Internet-Datenverkehr, der Dateischutz und die Untersuchung Ihres Computers korrekt funktionieren.

Denken Sie unbedingt daran, den Virenschutz für den Internet-Datenverkehr und den Virenschutz für Dateien wieder zu aktivieren, nachdem die Überprüfung mit der EICAR-Testdatei abgeschlossen wurde.

➡ *Gehen Sie folgendermaßen vor, um den Schutz für den Internet-Datenverkehr unter Verwendung der EICAR-Testdatei zu überprüfen:*

1. Laden Sie die EICAR-Testdatei von der offiziellen Webseite der EICAR-Organisation herunter: http://www.eicar.org/anti_virus_test_file.htm.

2. Versuchen Sie, die EICAR-Testdatei in einem beliebigen Ordner auf Ihrem Computer zu speichern.

Kaspersky Internet Security meldet, dass unter der angeforderten URL-Adresse eine Bedrohung gefunden wurde, und blockiert die Speicherung des Objekts auf dem Computer.

3. Verwenden Sie bei Bedarf verschiedene Typen der EICAR-Testdatei (s. Abschnitt "Über die Typen der EICAR-Testdatei" auf S. 188).

Gehen Sie folgendermaßen vor, um den Dateischutz unter Verwendung der EICAR-Testdatei oder eines Typs der Testdatei zu überprüfen::

1. Halten Sie den Virenschutz für den Internet-Datenverkehr und den Virenschutz für Dateien auf Ihrem Computer an.

   Es wird davor gewarnt, den Computer an lokale Netzwerke anzuschließen oder Wechseldatenträger zu verwenden, während der Schutz angehalten ist. Andernfalls können Schadprogramme Ihren Computer beschädigen.

2. Laden Sie die EICAR-Testdatei von der offiziellen Webseite des EICAR-Instituts herunter: http://www.eicar.org/anti_virus_test_file.htm.

3. Speichern Sie die EICAR-Testdatei in einem beliebigen Ordner auf Ihrem Computer.

4. Fügen Sie am Zeilenanfang der EICAR-Testdatei ein Präfix hinzu (s. Abschnitt "Über die Typen der EICAR-Testdatei" auf S. 188).

   Dafür eignet sich ein beliebiger Text- oder Hypertext-Editor (beispielsweise Editor). Gehen Sie auf **Start** → **Programme** → **Zubehör** → **Editor**, um den Editor zu starten.

5. Speichern Sie die so entstandene Datei unter einem Namen, der über den Typ der EICAR-Testdatei Aufschluss gibt: Speichern Sie beispielsweise eine Datei, in der das Präfix DELE- hinzugefügt wurde, unter dem Namen eicar_dele.com.

6. Aktivieren Sie den Virenschutz für den Internet-Datenverkehr und den Virenschutz für Dateien auf Ihrem Computer wieder.

7. Versuchen Sie, die gespeicherte Datei zu starten.

   Kaspersky Internet Security meldet, dass auf der Festplatte Ihres Computers eine Bedrohung gefunden wurde, und führt die Aktion aus, die in den Einstellungen des Dateischutzes festgelegt ist.

Gehen Sie folgendermaßen vor, um die Virensuche unter Verwendung der EICAR-Testdatei oder eines Typs der Testdatei zu überprüfen::

1. Halten Sie den Virenschutz für den Internet-Datenverkehr und den Virenschutz für Dateien auf Ihrem Computer an.

   Es wird davor gewarnt, den Computer an lokale Netzwerke anzuschließen oder Wechseldatenträger zu verwenden, während der Schutz angehalten ist. Andernfalls können Schadprogramme Ihren Computer beschädigen.

2. Laden Sie die EICAR-Testdatei von der offiziellen Webseite des EICAR-Instituts herunter: http://www.eicar.org/anti_virus_test_file.htm.

3. Fügen Sie am Zeilenanfang der EICAR-Testdatei ein Präfix hinzu (s. Abschnitt "Über die Typen der EICAR-Testdatei" auf S. 188).

   Dafür eignet sich ein beliebiger Text- oder Hypertext-Editor (beispielsweise Editor). Gehen Sie auf **Start** → **Programme** → **Zubehör** → **Editor**, um den Editor zu starten.

4. Speichern Sie die so entstandene Datei unter einem Namen, der über den Typ der EICAR-Testdatei Aufschluss gibt: Speichern Sie beispielsweise eine Datei, in der das Präfix DELE- hinzugefügt wurde, unter dem Namen eicar_dele.com.

5. Starten Sie eine Untersuchung der gespeicherten Datei.

Kaspersky Internet Security meldet, dass auf der Festplatte Ihres Computers eine Bedrohung gefunden wurde, und führt die Aktion aus, die in den Untersuchungseinstellungen für den Computer festgelegt ist.

6. Aktivieren Sie den Virenschutz für den Internet-Datenverkehr und den Virenschutz für Dateien auf Ihrem Computer wieder.

ÜBER DIE TYPEN DER EICAR-TESTDATEI

Sie können unterschiedliche Typen der EICAR-Testdatei erstellen, um die Programmfunktionen zu überprüfen. Das Programm erkennt die von Ihnen erstellte EICAR-Testdatei (die Variante) und weist ihr abhängig vom Untersuchungsergebnis einen Status zu. Das Programm führt mit der EICAR-Testdatei die Aktionen aus, die in den Einstellungen der Komponente festgelegt sind, von der die EICAR-Testdatei gefunden wurde.

Die erste Tabellenspalte (s. folgende Tabelle) enthält Präfixe, mit denen Sie Varianten der EICAR-Testdatei erstellen können. Die zweite Spalte zeigt die möglichen Werte für den Status, den eine Datei aufgrund der Untersuchungsergebnisse erhalten kann. Die dritte Spalte informiert darüber, wie Dateien mit dem betreffenden Status vom Programm verarbeitet werden.

Tabelle 2. Typen der EICAR-Testdatei

Präfix	Dateistatus	Informationen zur Verarbeitung einer Datei
Kein Präfix, standardmäßiger Testvirus.	**Infiziert**. Die Datei enthält einen bekannten Viruscode. Eine Desinfektion der Datei ist nicht möglich.	Das Programm identifiziert diese Datei als Datei, die einen Virus enthält, der nicht desinfiziert werden kann. Beim Desinfektionsversuch der Datei wird die Aktion ausgeführt, die für infizierte Dateien gilt. Standardmäßig zeigt das Programm eine Meldung darüber an, dass die infizierte Datei nicht desinfiziert werden kann.
CURE-	**Infiziert**. Die Datei enthält einen bekannten Viruscode. Eine Desinfektion der Datei ist möglich.	Die Datei enthält einen Virus, der desinfiziert oder gelöscht werden kann. Das Programm desinfiziert die Datei. Dabei wird der Text des Viruskörpers in CURE geändert. Das Programm zeigt eine Meldung über den Fund einer infizierten Datei an.
DELE-	**Infiziert**. Die Datei enthält einen bekannten Viruscode. Eine Desinfektion der Datei ist nicht möglich.	Das Programm identifiziert diese Datei als Virus, der nicht desinfiziert werden kann, und löscht die Datei. Das Programm zeigt eine Meldung über das Löschen einer infizierten Datei an.
WARN-	**Möglicherweise infiziert**. Die Datei enthält einen unbekannten Viruscode. Eine Desinfektion der Datei ist nicht möglich.	Die Datei wird als möglicherweise infiziert eingestuft. Das Programm führt die Aktion mit der Datei aus, die für möglicherweise infizierte Dateien gilt. Standardmäßig zeigt das Programm eine Meldung über den Fund einer möglicherweise infizierten Datei an.
SUSP-	**Möglicherweise infiziert.** Die Datei enthält den modifizierten Code eines bekannten Virus. Eine Desinfektion der Datei ist nicht möglich.	Das Programm hat eine partielle Übereinstimmung des Dateicodes mit einem Codeabschnitt eines bekannten Virus erkannt. Im Augenblick des Funds einer möglicherweise infizierten Datei enthalten die Programm-Datenbanken keine Beschreibung für den vollständigen Code dieses Virus. Das Programm führt die Aktion mit der Datei aus, die für möglicherweise infizierte Dateien gilt. Standardmäßig zeigt das Programm eine Meldung über den Fund einer möglicherweise infizierten Datei an.
CORR-	**Beschädigt**.	Das Programm untersucht eine Datei dieses Typs nicht, weil die Dateistruktur beschädigt ist (z.B. ungültiges Dateiformat). Informationen darüber, dass die Datei verarbeitet wurde, können Sie dem Programmbericht entnehmen.
ERRO-	**Untersuchungsfehler**.	Bei der Untersuchung der Datei ist ein Fehler aufgetreten. Das Programm konnte nicht auf die Datei zugreifen: Die Integrität die Datei ist beschädigt (z.B. kein Endpunkt in einem Multi-Level-Archiv) oder eine Verbindung zu der Datei ist nicht möglich (wenn sich eine Datei auf einem Netzlaufwerk befindet). Informationen darüber, dass die Datei verarbeitet wurde, können Sie dem Programmbericht entnehmen.

KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Dieser Abschnitt beschreibt, wie Sie technische Unterstützung erhalten können und nennt die Voraussetzungen, die dafür erfüllt werden müssen.

IN DIESEM ABSCHNITT

WIE SIE TECHNISCHEN KUNDENDIENST ERHALTEN

Wenn Sie in der Programmdokumentation und in den Informationsquellen zum Programm (s. Abschnitt "Informationsquellen zum Programm" auf S. 14) keine Lösung für Ihr Problem finden können, empfehlen wir Ihnen, sich an den Technischen Support von Kaspersky Lab zu wenden. Die Support-Mitarbeiter beantworten Ihre Fragen zur Installation und Verwendung des Programms. Wenn Ihr Computer infiziert ist, helfen die Support-Experten Ihnen dabei, die Folgen schädlicher Malware-Aktionen zu beheben.

Bevor Sie sich an den technischen Support wenden, lesen Sie sich zuvor die Supportrichtlinien (http://support.kaspersky.de/support/rules) durch.

Eine Kontaktaufnahme mit den Support-Experten ist auf folgende Weise möglich:

- Telefonisch. Sich können sich am Telefon von den Spezialisten des lokalen oder internationalen Technischen Supports beraten lassen.
- Aus Mein Kaspersky Account auf der Support-Webseite eine Anfrage senden. Sich können sich über ein Webformular an die Support-Experten wenden.

Sie müssen registrierter Benutzer von Kaspersky Internet Security sein, um die technische Unterstützung nutzen zu können. Für Testversionen des Programms wird keine technische Unterstützung gewährt.

PROTOKOLLDATEI UND AVZ-SKRIPT VERWENDEN

Wenn Sie sich mit einem Problem an den Technischen Support wenden, bitten die Support-Experten Sie möglicherweise darum, einen Bericht über den Systemzustand zu erstellen und den Bericht an den Technischen Support zu schicken. Zusätzlich können die Support-Experten eine *Protokolldatei* anfordern. Eine Protokolldatei ermöglicht eine schrittweise Prüfung von ausgeführten Programmbefehlen. Dadurch lässt sich erkennen, auf welcher Etappe ein Fehler aufgetreten ist.

Aufgrund einer Analyse der von Ihnen eingesandten Daten können die Support-Experten ein AVZ-Skript erstellen, das dann an Sie geschickt wird. Mit Hilfe von AVZ-Skripten können die laufenden Prozesse auf schädlichen Code analysiert, das System auf schädlichen Code untersucht, infizierte Dateien desinfiziert / gelöscht, und ein Bericht über die Ergebnisse der Systemuntersuchung erstellt werden.

BERICHT ÜBER DEN SYSTEMZUSTAND ERSTELLEN

Gehen Sie folgendermaßen vor, um einen Bericht über den Systemzustand zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.
3. Klicken Sie im folgenden Fenster **Protokollierung** auf **Bericht über den Systemstatus erstellen**.

Der Bericht über den Systemzustand wird in den Formaten html und xml erstellt und im Archiv sysinfo.zip gespeichert. Nachdem das Sammeln von Daten über das System abgeschlossen wurde, können Sie einen Bericht ansehen.

Gehen Sie folgendermaßen vor, um einen Bericht anzuzeigen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.
3. Klicken Sie im folgenden Fenster **Protokollierung** auf die Schaltfläche **Anzeigen**.
4. Öffnen Sie das Archiv sysinfo.zip, das die Protokolldateien enthält.

PROTOKOLLDATEI ERSTELLEN

Gehen Sie folgendermaßen vor, um eine Protokolldatei zu erstellen:

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.
3. Wählen Sie im folgenden Fenster **Protokollierung** im Block **Protokollierung** aus der Dropdown-Liste ein Protokollierungsniveau.

   Es wird empfohlen, die Support-Experten nach dem erforderlichen Tracing-Niveau zu fragen. Sollte diese Angabe des Supports fehlen, dann empfohlen, das Tracing-Niveau **500** einzustellen.
4. Klicken Sie auf **Aktivieren**, um den Protokollierungsvorgang zu starten.
5. Wiederholen Sie die Situation, in der das Problem aufgetreten ist.
6. Klicken Sie auf **Deaktivieren**, um den Protokollierungsvorgang zu beenden.

Sie können mit dem Hochladen der Protokollierungsergebnisse (s. Abschnitt "Datendateien versenden" auf S. 191) auf den Server von Kaspersky Lab beginnen.

DATEIEN MIT DATEN SENDEN

Nachdem die Protokolldateien und der Bericht über den Systemzustand erstellt wurden, müssen diese an den Technischen Support von Kaspersky Lab geschickt werden.

Um die Dateien mit den Daten auf den Server des Technischen Supports hochzuladen, benötigen Sie eine Anfragenummer. Diese Nummer erhalten Sie in Ihrem Kaspersky Account auf der Webseite des Technischen Supports, wenn eine aktive Anfrage vorliegt.

➡ *Gehen Sie folgendermaßen vor, um die Dateien mit den Daten auf den Server des Technischen Supports hochzuladen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.
3. Klicken Sie im folgenden Fenster **Protokollierung** im Block **Aktionen** auf **Informationen für den Support auf den Server laden**.

   Das Fenster **Support-Informationen auf Server hochladen** wird geöffnet.
4. Aktivieren Sie die Kontrollkästchen neben den Dateien, die Sie an den Technischen Support schicken möchten, und klicken Sie auf **Senden**.

   Das Fenster **Anfragenummer** wird geöffnet.
5. Geben Sie die Nummer an, die Ihre Anfrage in Mein Kaspersky Account vom Technischen Support erhalten hat, und klicken Sie auf **OK**.

Die gewählten Dateien werden komprimiert und an den Server des Technischen Supports gesendet.

Falls kein Kontakt mit dem Technischen Support möglich ist, können Sie diese Dateien auf Ihrem Computer speichern und sie später aus Mein Kaspersky Account absenden.

➡ *Gehen Sie folgendermaßen vor, um die Dateien mit Daten auf der Festplatte zu speichern:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.
3. Klicken Sie im folgenden Fenster **Protokollierung** im Block **Aktionen** auf **Informationen für den Support auf den Server laden**.

   Das Fenster **Support-Informationen auf Server hochladen** wird geöffnet.
4. Aktivieren Sie die Kontrollkästchen neben den Dateien, die Sie an den Technischen Support schicken möchten, und klicken Sie auf **Senden**.

   Das Fenster **Anfragenummer** wird geöffnet.
5. Klicken Sie auf **Abbrechen** und bestätigen Sie im folgenden Fenster mit **Ja**, dass die Dateien auf der Festplatte gespeichert werden.

   Ein Fenster zum Speichern des Archivs wird geöffnet.
6. Geben Sie einen Namen für das Archiv an und bestätigen Sie das Speichern.

Das fertige Archiv können Sie über Mein Kaspersky Account an den Technischen Support senden.

AVZ-SKRIPT AUSFÜHREN

Es wird davor gewarnt, den Text eines Skripte, das Ihnen von den Support-Spezialisten geschickt wurde, zu verändern. Sollten bei der Skript-Ausführung Probleme auftreten, dann wenden Sie sich an den technischen Support (s. Abschnitt "Wie Sie technischen Kundendienst erhalten" auf S. 190).

➡ *Gehen Sie folgendermaßen vor, um ein AVZ-Skript auszuführen:*

1. Öffnen Sie das Programmhauptfenster.
2. Klicken Sie im unteren Bereich des Hauptfensters auf **Support**, um das Fenster **Support** zu öffnen, und klicken Sie dort auf den Link **Protokollierung**.
3. Klicken Sie im folgenden Fenster **Protokollierung** auf die Schaltfläche **AVZ-Skript ausführen**.

Wenn das Skript erfolgreich ausgeführt wurde, wird der Assistent abgeschlossen. Falls bei der Skript-Ausführung Störungen auftreten, zeigt der Assistent eine entsprechende Meldung an.

TECHNISCHER SUPPORT AM TELEFON

Bei dringenden Problemen können Sie jederzeit den lokalen oder internationalen Technischen Support anrufen (http://support.kaspersky.de/support/support_local).

Wenn Sie sich an den Technischen Support wenden möchten, halten Sie bitte die erforderlichen Informationen (http://support.kaspersky.ru/support/details) über Ihren Computer und die installierten Antiviren-Programme bereit. Dadurch können unsere Spezialisten Ihnen möglichst schnell helfen.

TECHNISCHEN SUPPORT ERHALTEN ÜBER MEIN KASPERSKY ACCOUNT

Mein Kaspersky Account ist Ihr persönlicher Bereich https://my.kaspersky.de/ auf der Seite des Technischen Supports.

Sie müssen sich auf der Login-Seite anmelden (https://my.kaspersky.com/de/registration). Geben Sie Ihre E-Mail-Adresse und das Kennwort für den Zugriff auf Ihren Kaspersky Account an.

In Mein Kaspersky Account können Sie folgende Aktionen ausführen:

- Anfragen an den Technischen Support und an das Virenlabor senden.
- mit dem Technischen Support kommunizieren, ohne ohne E-Mails zu verwenden.
- Status Ihrer Anfragen in Echtzeit verfolgen.
- vollständigen Verlauf Ihrer Anfragen an den Technischen Support ansehen.

E-Mail-Anfrage an den Technischen Support

Anfragen an den Technischen Support können per E-Mail auf Deutsch, Englisch, Französisch, Spanisch oder Russisch gestellt werden.

Füllen Sie folgende Felder des elektronischen Formulars aus:

- Typ der Anfrage.
- Name und Versionsnummer des Programms.
- Anfragetext.
- Kundennummer und Kennwort.
- E-Mail-Adresse.

Die Support-Spezialisten richten ihre Antwort an Mein Kaspersky Account und an die E-Mail-Adresse, die in der Anfrage angegeben wurde.

Elektronische Anfrage an das Virenlabor

Beachten Sie, dass für die Bearbeitung bestimmter Anfragen nicht der Technische Support, sondern das Virenlabor verantwortlich ist.

Sie können folgende Anfragetypen an das Virenlabor richten:

- *Unbekanntes Schadprogramm* – Sie haben den Verdacht, dass eine Datei einen Virus enthält, obwohl Kaspersky Internet Security sie nicht als infiziert einstuft.

  Die Experten des Virenlabors analysieren den eingeschickten Schadcode. Wird ein bisher unbekannter Virus gefunden, so wird seine Beschreibung einer Datenbank hinzugefügt, die bei der nächsten Aktualisierung der Antiviren-Programme verfügbar gemacht wird.

- *Viren-Fehlalarm* – Kaspersky Internet Security stuft eine Datei als infiziert ein, während Sie sicher sind, dass die Datei virenfrei ist.

- *Anfrage für eine Beschreibung eines Schadprogramms* – Sie möchten auf Basis des Virusnamens die Beschreibung eines bestimmten Virus erhalten, den Kaspersky Internet Security gefunden hat.

Anfragen an das Virenlabor können Sie auf der Seite (http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de) stellen. Dazu ist keine Anmeldung bei Mein Kaspersky Account notwendig. In diesem Fall ist die Angabe eines Aktivierungscodes notwendig.

ANHÄNGE

Dieser Abschnitt enthält Informationen, die den Haupttext des Dokuments ergänzen.

IN DIESEM ABSCHNITT

BEDIENUNG DES PROGRAMMS ÜBER DIE BEFEHLSZEILE

Sie können Kaspersky Internet Security mit Hilfe der Befehlszeile steuern. Dabei ist die Möglichkeit zum Ausführen der folgenden Operationen vorgesehen:

- Programm aktivieren
- Programm starten und beenden
- Programmkomponenten starten und beenden.
- Aufgaben starten und beenden
- Erhalt von Informationen über den aktuellen Status von Komponenten und Aufgaben und ihrer Statistik.
- Ausführung von Untersuchungsaufgaben starten und beenden.
- Untersuchung von ausgewählten Objekten.
- Update der Datenbanken und Programm-Module, Rollback von Updates.
- Export und Import von Schutzeinstellungen.
- Aufruf der Hilfe über die Syntax der Befehlszeile insgesamt und für einzelne Befehle.

Syntax der Befehlszeile:

```
avp.com <Befehl> [Parameter]
```

Der Zugriff auf das Programm über die Befehlszeile muss aus dem Installationsordner des Produkts oder unter Angabe des vollständigen Pfads von avp.com erfolgen.

Die Liste der Befehle, die für die Steuerung des Programms und seiner Komponenten verwendet werden, finden Sie in der nachstehenden Tabelle.

START	Komponente oder Aufgabe starten.
STOP	Komponente oder Aufgabe beenden (Dieser Befehl ist nur möglich, wenn das über die Oberfläche von Kaspersky Internet Security festgelegte Kennwort eingegeben wird).
STATUS	Aktuellen Status einer Komponente oder Aufgabe auf dem Bildschirm anzeigen.
STATISTICS	Statistik über die Arbeit einer Komponente oder Aufgabe auf dem Bildschirm anzeigen.
HELP	Befehlsliste und Informationen zur Befehlssyntax auf dem Bildschirm anzeigen.

SCAN	Objekte auf das Vorhandensein von Viren untersuchen.
UPDATE	Programm-Update starten.
ROLLBACK	Rückgängigmachen des zuletzt ausgeführten Updates von Kaspersky Internet Security (Dieser Befehl ist nur möglich, wenn das über die Programmoberfläche festgelegte Kennwort eingegeben wird).
EXIT	Beenden der Arbeit mit dem Programm (Dieser Befehl ist nur möglich, wenn das über die Programmoberfläche festgelegte Kennwort eingegeben wird).
IMPORT	Schutzeinstellungen für Kaspersky Internet Security importieren (Dieser Befehl ist nur möglich, wenn das über die Programmoberfläche festgelegte Kennwort eingegeben wird).
EXPORT	Schutzeinstellungen des Programms exportieren.

Jedem Befehl entspricht eine eigene Auswahl von Parametern, die für eine konkrete Komponente des Programms spezifisch sind.

IN DIESEM ABSCHNITT

PROGRAMM AKTIVIEREN

Kaspersky Internet Security kann mit Hilfe einer Schlüsseldatei aktiviert werden.

Befehlssyntax:

```
avp.com ADDKEY <Dateiname>
```

Eine Beschreibung der Parameter für die Befehlsausführung ist in der nachstehenden Tabelle zu finden.

<Dateiname>	Name eines Lizenzschlüssels mit der Endung key.

Beispiel:

```
avp.com ADDKEY 1AA111A1.key
```

PROGRAMM STARTEN

Befehlssyntax:

```
avp.com
```

PROGRAMM BEENDEN

Befehlssyntax:

```
avp.com EXIT /password=<Kennwort>
```

Folgende Tabelle beschreibt die Parameter.

<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

STEUERUNG VON KOMPONENTEN UND AUFGABEN DES PROGRAMMS

Befehlssyntax:

```
avp.com <Befehl> <Profil|Aufgabenname> [/R[A]:<Berichtsdatei>]
avp.com STOP <Profil|Aufgabenname> /password=<Kennwort> [/R[A]:<Berichtsdatei>]
```

Befehle und Parameter werden in folgender Tabelle beschrieben.

<Befehl>	Die Steuerung der Komponenten und Aufgaben von Kaspersky Internet Security wird mit Hilfe der folgenden Befehle ausgeführt: START – Start einer Schutzkomponente oder einer Aufgabe. STOP – Beenden einer Schutzkomponente oder einer Aufgabe. STATUS – Aktuellen Status einer Komponente oder Aufgabe auf dem Bildschirm anzeigen. STATISTICS – Die Statistik über die Arbeit einer Schutzkomponente oder einer Aufgabe auf dem Bildschirm anzeigen. Beachten Sie, dass der Befehl STOP nur ausgeführt wird, wenn das Kennwort eingegeben wird.
<Profil|Aufgabenname>	Als Wert für den Parameter **<Profil>** sind möglich: kann eine beliebige Schutzkomponente von Kaspersky Internet Security, Module, die zu den Komponenten gehören, erstellte Untersuchungs- oder Updateaufgaben (die vom Programm standardmäßig verwendeten Werte werden in folgender Tabelle genannt) angegeben werden. Als Wert für den Parameter **<Aufgabenname>** kann der Name einer beliebigen vom Benutzer erstellten Untersuchungs- oder Updateaufgabe angegeben werden.
<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.
/R[A]:<Berichtsdatei>	**/R:<Berichtsdatei>** – Nur wichtige Ereignisse im Bericht erfassen. **/RA:<Berichtsdatei>** – Alle Ereignisse im Bericht erfassen. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.

Für den Parameter **<Profil>** wird einer der Werte aus folgender Tabelle angegeben.

RTP	Alle Schutzkomponenten. Der Befehl **avp.com START RTP** startet alle Schutzkomponenten, wenn der Schutz vollständig deaktiviert war. Wenn eine Komponente mit dem Befehl **STOP** aus der Befehlszeile beendet wurde, wird sie durch den Befehl **avp.com START RTP** nicht gestartet. Um eine Komponente zu starten, muss der Befehl **avp.com START <Profil>** ausgeführt werden. Dabei wird für **<Profil>** der Wert einer konkreten Schutzkomponente eingesetzt, beispielsweise **avp.com START FM**.
FW	Firewall.
HIPS	Programmkontrolle aus.
pdm	Proaktiver Schutz.
FM	Datei-Anti-Virus.
EM	Mail-Anti-Virus.
WM	Web-Anti-Virus. Werte für die Subkomponenten von Web-Anti-Virus: **httpscan (HTTP)** – Untersuchung des http-Datenstroms **sc** – Skript-Untersuchung
IM	IM-Anti-Virus.
AB	Anti-Banner
AS	Anti-Spam.
PC	Kindersicherung.
AP	Anti-Phishing.
ids	Schutz vor Netzwerkangriffen.
Updater	Update.
Rollback	Rollback zum vorherigen Update.
Scan_My_Computer	Untersuchung des Computers.
Scan_Objects	Objekte untersuchen.
Scan_Quarantine	Quarantäne untersuchen.
Scan_Startup (STARTUP)	Autostart-Objekte untersuchen.
Scan_Vulnerabilities (SECURITY)	Schwachstellensuche.

Die aus der Befehlszeile gestarteten Komponenten und Aufgaben werden mit den Parametern ausgeführt, die über die Programmoberfläche festgelegt wurden.

Beispiele:

➨ *Geben Sie folgenden Befehl ein, um Datei-Anti-Virus zu aktivieren:*

```
avp.com START FM
```

➡ *Geben Sie folgenden Befehl ein, um die Untersuchung des Computers abzubrechen:*

```
avp.com STOP Scan_My_Computer /password=<Kennwort>
```

VIRENSUCHE

Die Befehlszeile zum Starten der Virenuntersuchung eines bestimmten Bereichs und zum Starten der Verarbeitung von schädlichen Objekten besitzt folgendes allgemeines Aussehen:

```
avp.com SCAN [<Untersuchungsobjekt>] [<Aktion>] [<Dateitypen>] [<Ausnahmen>]
[<Konfigurationsdatei>] [<Berichtsparameter>] [<zusätzliche Parameter>]
```

Für die Untersuchung von Objekten können Sie auch die im Programm erstellten Aufgaben verwenden, die aus der Befehlszeile gestartet werden können. Dabei wird die Aufgabe mit den Parametern ausgeführt, die über die Oberfläche von Kaspersky Internet Security festgelegt wurden.

Folgende Tabelle beschreibt die Parameter.

<Untersuchungsobjekt> – Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
<files>	Liste mit den Pfaden der Dateien und Ordner für die Untersuchung. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen. Kommentare: • Wenn der Objektname ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt. • Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.
/MEMORY	Objekte des Arbeitsspeichers.
/STARTUP	Autostart-Objekte**.**
/MAIL	Posteingänge.
/REMDRIVES	Alle Wechseldatenträger.
/FIXDRIVES	Alle lokalen Laufwerke.
/NETDRIVES	Alle Netzlaufwerke.
/QUARANTINE	Objekte in Quarantäne.
/ALL	Vollständige Untersuchung des Computers.
/@:<filelist.lst>	Pfad der Datei mit einer Liste der Objekte und Ordner, die untersucht werden sollen. Für die Datei mit der Liste ist die Angabe des absoluten oder relativen Pfads zulässig. Der Pfad wird ohne Anführungszeichen angegeben, selbst wenn er ein Leerzeichen enthält. Die Datei mit der Liste muss das Textformat besitzen. Jedes Untersuchungsobjekt muss in einer separaten Zeile stehen. Es wird empfohlen, in der Datei die absoluten Pfade der Untersuchungsobjekte anzugeben. Bei Angabe eines relativen Pfads wird der Pfad im Bezug auf die ausführbare Programmdatei angegeben, nicht im Bezug auf die Datei mit der Liste der Untersuchungsobjekte.

<Aktion> – Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert **/i8** entspricht. Wenn Sie im automatischen Modus arbeiten, wendet Kaspersky Internet Security beim Fund gefährlicher Objekte automatisch die von Kaspersky Lab empfohlene Aktion an. Die Aktion ausgeführt, die dem **<Aktion>** entspricht, wird ignoriert.	
/i0	Keine Aktion ausführen, Informationen im Bericht protokollieren.
/i1	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen**.**
/i2	Infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; infizierte Objekte aus Containern (zusammengesetzten Objekten) nicht löschen; Container mit ausführbarer Kopfzeile (sfx-Archive) löschen.
/i3	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i4	infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i8	Beim Fund eines infizierten Objekts den Benutzer nach der Aktion fragen.
/i9	Den Benutzer nach der Aktion fragen, wenn die Untersuchung abgeschlossen wird.
<Dateitypen> – Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht.	
/fe	Nur infizierbare Dateien nach Erweiterung untersuchen.
/fi	Nur infizierbare Dateien nach Inhalt untersuchen.
/fa	**Alle Dateien untersuchen**.
<Ausnahmen> – Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen. Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.	
-e:a	Archive nicht untersuchen.
-e:b	Mail-Datenbanken nicht untersuchen.
-e:m	E-Mail-Nachrichten im Format plain text nicht untersuchen.
-e:<filemask>	Objekte nach Maske nicht untersuchen.
-e:<seconds>	Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter **<seconds>** angegebene Zeitraum.
-es:<size>	Objekte überspringen, deren Größe (in MB) über dem Wert liegt, der durch den Parameter **<size>** angegeben wird. Der Parameter ist nur auf zusammengesetzte Dateien (z.B. Archive) anwendbar.
<Konfigurationsdatei> – Bestimmt den Pfad einer Konfigurationsdatei mit den Programmeinstellungen, die für eine Untersuchung gelten. Die Konfigurationsdatei ist eine Datei im Textformat, die eine Auswahl von Befehlszeilenparametern für die Antiviren-Untersuchung enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.	
/C:<Dateiname>	Die Werte der Parameter, die in der Datei **<Dateiname>** angegeben sind, verwenden.

<Berichtsparameter> – Dieser Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.	
/R:<Berichtsdatei>	Nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
/RA:<Berichtsdatei>	Alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren.
<zusätzliche Parameter> – Parameter, der die Verwendung von Technologien zur Virenuntersuchung festlegt.	
/iChecker=<on|off>	Verwendung der Technologie iChecker aktivieren / deaktivieren.
/iSwift=<on|off>	Verwendung der Technologie iSwift aktivieren / deaktivieren.

Beispiele:

- *Untersuchung des Arbeitsspeichers, der Autostart-Objekte, der Mailboxen sowie der Ordner Eigene Dateien, Programme und der Datei test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\My
Documents" "C:\Program Files" "C:\Downloads\test.exe"
```

- *Untersuchung der Objekte, deren Liste in der Datei object2scan.txt angegeben ist. Für die Arbeit soll die Konfigurationsdatei scan_settings.txt verwendet werden. Über die Untersuchungsergebnisse soll ein Bericht erstellt werden, in dem alle Ereignisse aufgezeichnet werden:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Beispiel für die Konfigurationsdatei:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

PROGRAMM-UPDATE

Der Befehl für das Update der Programm-Module und Datenbanken von Kaspersky Internet Security besitzt folgende Syntax:

```
avp.com UPDATE [<Updatequelle>] [/R[A]:<Berichtsdatei>] [/C:<Dateiname>]
```

Folgende Tabelle beschreibt die Parameter.

<Updatequelle>	HTTP-, FTP-Server oder Netzwerkordner für den Download von Updates. Als Wert für diesen Parameter kann der vollständige Pfad oder die URL-Adresse der Updatequelle angegeben werden. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Parametern des Diensts für das Programm-Update übernommen.
/R[A]:<Berichtsdatei>	**/R:**<Berichtsdatei> – nur wichtige Ereignisse im Bericht protokollieren. **/RA:**<Berichtsdatei> - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.
/C:<Dateiname>	Pfad der Konfigurationsdatei, die die Parameter für die Arbeit von Kaspersky Internet Security beim Update enthält. Die Konfigurationsdatei ist eine Textdatei, die eine Auswahl von Befehlszeilenparametern für das Update des Programms enthält. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die über die Programmoberfläche festgelegt wurden.

Beispiele:

➡ *Update der Programm-Datenbanken, alle Ereignisse im Bericht protokollieren:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

➡ *Update der Programm-Module von Kaspersky Internet Security, die Parameter der Konfigurationsdatei updateapp.ini verwenden:*

```
avp.com UPDATE /C:updateapp.ini
```

Beispiel für die Konfigurationsdatei:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK ZUM VORHERIGEN UPDATE

Befehlssyntax:

```
avp.com ROLLBACK [/R[A]:<Berichtsdatei>][/password=<Kennwort>]
```

Folgende Tabelle beschreibt die Parameter.

/R[A]:<Berichtsdatei>	**/R:**<Berichtsdatei> – nur wichtige Ereignisse im Bericht protokollieren. **/RA:**<Berichtsdatei> - alle Ereignisse im Bericht protokollieren. Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.
<Kennwort>	Kennwort für das Programm, das über die Programmoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

Beispiel:

```
avp.com ROLLBACK /RA:rollback.txt /password=<Kennwort>
```

SCHUTZPARAMETER EXPORTIEREN

Befehlssyntax:

```
avp.com EXPORT <Profil> <Dateiname>
```

Eine Beschreibung der Parameter für die Befehlsausführung ist in der nachstehenden Tabelle zu finden.

<Profil>	Komponente oder Aufgabe, für die der Export von Parametern ausgeführt wird. Als Wert des Parameters **<Profil>** kann ein beliebiger Wert dienen, der im Hilfeabschnitt "Steuerung von Komponenten und Aufgaben des Programms" genannt wird.
<Dateiname>	Pfad der Datei, in welche die Parameter von Kaspersky Internet Security exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden. Die Konfigurationsdatei wird im Binärformat (dat) gespeichert und kann künftig verwendet werden, um die Einstellungen des Programms auf andere Computer zu übertragen. Außerdem können Sie die Konfigurationsdatei im Textformat speichern. Geben Sie dazu im Dateinamen die Endung txt an. Beachten Sie, dass der Import von Schutzparametern aus einer Textdatei nicht unterstützt wird. Diese Datei kann nur zur Ansicht der grundlegenden Funktionsparameter von Kaspersky Internet Security verwendet werden.

Beispiel:

```
avp.com EXPORT RTP c:\settings.dat
```

SCHUTZPARAMETER IMPORTIEREN

Befehlssyntax:

```
avp.com IMPORT <Dateiname> [/password=<Kennwort>]
```

Eine Beschreibung der Parameter für die Befehlsausführung ist in der nachstehenden Tabelle zu finden.

<Dateiname>	Pfad der Datei, aus welcher die Parameter von Kaspersky Internet Security importiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.
<Kennwort>	Kennwort für Kaspersky Internet Security, das über die Programmoberfläche festgelegt wurde. <Kennwort>

Beachten Sie, dass dieser Befehl nicht ausgeführt wird, wenn das Kennwort nicht eingegeben wird.

Beispiel:

```
avp.com IMPORT c:\settings.dat /password=<Ihr_Kennwort>
```

PROTOKOLLDATEI ANLEGEN

Das Anlegen einer Protokolldatei kann erforderlich sein, wenn bei der Arbeit von Kaspersky Internet Security Probleme auftreten. Die Protokolldatei ermöglicht den Experten des Technischen Supports eine genaue Problemanalyse.

Es wird empfohlen, das Anlegen von Tracing-Dateien nur zur Diagnose eines konkreten Problems zu aktivieren. Sollte das Tracing ständig aktiv sein, so kann die Leistungsfähigkeit des Computers sinken und es kann zur Überfüllung der Festplatte kommen.

Befehlssyntax:

```
avp.com TRACE [file] [on|off] [<Tracing-Niveau>]
```

Folgende Tabelle beschreibt die Parameter.

[on|off]	Anlegen einer Protokolldatei aktivieren / deaktivieren.
[file]	Tracing in Form einer Datei erstellen.
<Tracing-Niveau>	Für diesen Parameter kann ein Zahlenwert im Bereich von 0 (minimale Stufe, nur kritische Meldungen) bis 700 (maximale Stufe, alle Meldungen) festgelegt werden. Wenn Sie sich an den Technischen Support wenden, nennt Ihnen der zuständige Spezialist das erforderliche Tracing-Niveau. Andernfalls gilt das Niveau 500 als empfehlenswert.

Beispiele:

- *Erstellen von Protokolldateien deaktivieren:*

```
avp.com TRACE file off
```

- *Erstellen einer Protokolldatei mit dem maximalen Tracing-Niveau von 500. Diese Datei wird an den Technischen Support gesendet:*

```
avp.com TRACE file on 500
```

HILFE ANZEIGEN

Folgender Befehl dient zur Anzeige von Hilfeinformationen über die Syntax der Befehlszeile:

```
avp.com [ /? | HELP ]
```

Um Hilfeinformationen über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
avp.com <Befehl> /?
avp.com HELP <Befehl>
```

RÜCKGABECODES DER BEFEHLSZEILE

In diesem Abschnitt werden die Rückgabecodes der Befehlszeile beschrieben (s. folgende Tabelle). Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Als Rückgabecodes für Aufgaben sind die allgemeinen Codes sowie spezifische Codes für einen konkreten Aufgabentyp möglich.

ALLGEMEINE RÜCKGABECODES	
0	Die Operation wurde erfolgreich ausgeführt.
1	Ungültiger Parameterwert.
2	Unbekannter Fehler.
3	Fehler bei der Ausgabenausführung.
4	Die Aufgabenausführung wurde abgebrochen.
RÜCKGABECODES FÜR AUFGABEN ZUR VIRENSUCHE	
101	Alle gefährlichen Objekte wurden verarbeitet.
102	Es wurden gefährliche Objekte gefunden.

LISTE DER BENACHRICHTIGUNGEN VON KASPERSKY INTERNET SECURITY

Dieser Abschnitt informiert über die Benachrichtigungen, die während der Arbeit von Kaspersky Internet Security auf dem Bildschirm angezeigt werden können.

IN DIESEM ABSCHNITT

MELDUNGEN IN ALLEN SCHUTZMODI

Dieser Abschnitt enthält alle Meldungen, die sowohl im automatischen als auch im interaktiven Schutzmodus erscheinen können (s. Abschnitt "Schutzmodus auswählen" auf S. 68).

IN DIESEM ABSCHNITT

SPEZIELLE DESINFEKTIONSPROZEDUR IST ERFORDERLICH

Beim Fund einer Bedrohung, die gerade im System aktiv ist (beispielsweise schädlicher Prozess im Arbeitsspeicher oder in Autostart-Objekten) fordert eine Meldung dazu auf, eine speziell dafür vorgesehene erweiterte Desinfektionsprozedur durchzuführen.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Art der Bedrohung und Name des schädlichen Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines schädlichen Objekts befindet sich das Symbol ⓘ. Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung erhalten können, die dieses Objekt darstellt.

- Dateiname und Pfad eines schädlichen Objekts.

Folgende Aktionen stehen zur Auswahl:

- **Ja, bei Neustart desinfizieren** – Spezielle Desinfektionsprozedur ausführen (empfohlen).

  Während der Desinfektion werden alle Programme außer den vertrauenswürdigen blockiert. Zum Abschluss der Desinfektion wird das Betriebssystem neu gestartet. Deshalb sollten vor der Desinfektion die aktuellen Arbeitsergebnisse gespeichert und alle Programme geschlossen werden. Nach dem Neustart des Computers wird empfohlen, die vollständige Virenuntersuchung zu starten.

- **Nicht ausführen** – Das gefundene Objekt oder der Prozess wird entsprechend der zuvor gewählten Aktion verarbeitet.

Aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**, damit die gewählte Aktion immer in ähnlichen Situationen angewendet wird.

VERSTECKTES LADEN EINES TREIBERS

Bestimmte Schadprogramme laden heimlich Treiber auf einen PC. Anschließend lässt sich die Aktivität des Schadprogramms nicht mehr mit Kaspersky Internet Security kontrollieren. Diese Methode des Treiberdownloads wird nur selten von legalen Programmen verwendet.

Wenn die Programmkontrolle einen Versuch zum heimlichen Treiberdownload erkennt, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Name und Pfad der Treiberdatei

  Neben dem Dateinamen befindet sich das Symbol ⓘ. Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über den Treiber geöffnet.

Folgende Aktionen stehen zur Auswahl:

- **Jetzt erlauben** – Download des Treibers erlauben und Treiber zur Ausnahmeliste hinzufügen.
- **Jetzt verbieten** – Download des Treibers verbieten.
- **Quarantäne** – Download des Treibers verbieten und Treiberdatei in die Quarantäne verschieben.

EIN PROGRAMM OHNE DIGITALE SIGNATUR WIRD GESTARTET

Wenn die Programmkontrolle erkennt, dass auf dem Computer ein Programm gestartet wird, das keine digitale Signatur besitzt und das aufgrund einer heuristischen Analyse einen hohen Risikowert erhalten hat, so erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Name des zu startenden Programms

  Neben dem Namen des Programms befindet sich das Symbol . Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über das Programm geöffnet.

- Angaben über die Anzahl der Benutzer, die das Programm verwenden und ihm vertrauen.

Folgende Aktionen stehen zur Auswahl:

- **Ja, ich vertraue** – Start und Ausführung des Programms uneingeschränkt erlauben.
- **Programm beschränken** – Start des Programms erlauben, aber die Ausführung gefährlicher Operationen verbieten.
- **Blockieren** – Start und Ausführung des Programms jetzt und künftig verbieten.

EIN WECHSELDATENTRÄGER WURDE ANGESCHLOSSEN

Wenn ein Wechseldatenträger an den Computer angeschlossen wird, erscheint eine entsprechende Meldung auf dem Bildschirm.

Folgende Aktionen stehen zur Auswahl:

- **Schnelle Untersuchung** – Auf dem Wechseldatenträger die Dateien untersuchen, die ein potenzielles Risiko darstellen können.
- **Vollständige Untersuchung** – Alle Dateien auf dem Wechseldatenträger untersuchen.
- **Nicht untersuchen** – Wechseldatenträger nicht untersuchen.

Aktivieren Sie das Kontrollkästchen **In ähnlichen Fällen immer anwenden**, damit die gewählte Aktion künftig auf alle Wechseldatenträger angewendet wird, die angeschlossen werden.

NEUES NETZWERK WURDE GEFUNDEN

Bei jeder Verbindung des Computers mit einer neuen Zone (Netzwerk) erscheint eine Meldung auf dem Bildschirm.

Im Meldungsfenster werden oben Informationen zum Netzwerk genannt:

- Netzwerkadapter, der für die Netzwerkverbindung verwendet wird.
- Typ des Netzwerks (z.B. "drahtlos")
- Name des Netzwerks

Im unteren Bereich des Meldungsfensters können Sie einen Status für das gefundene Netzwerk festlegen, auf dessen Grundlage entschieden wird, welche Art von Netzwerkaktivität erlaubt wird:

- **Ja, das ist ein vertrauenswürdiges Netzwerk**. Es wird empfohlen, diesen Status nur für ein sicheres Netzwerk zu verwenden, in dem einem Computer keine Angriffe und unerlaubte Zugriffsversuche auf Daten drohen.
- **Lokales Netzwerk**. Es wird empfohlen, diesen Status für Netzwerke mit mittlerer Risikostufe anzuwenden (beispielsweise für ein internes Firmennetzwerk).

- **Nein, das ist ein öffentliches Netzwerk**. Netzwerk mit hoher Risikostufe. Bei der Arbeit in dieser Zone ist der Computer allen möglichen Typen von Bedrohungen ausgesetzt. Dieser Status wird auch für Netzwerke empfohlen, die nicht durch Antiviren-Programme, Firewalls und Filter geschützt sind. Die Auswahl dieses Status gewährleistet einem Computer bei der Arbeit im Netzwerk maximale Sicherheit.

EIN UNSICHERES ZERTIFIKAT WURDE GEFUNDEN

Kaspersky Internet Security überprüft die Zuverlässigkeit einer SSL-Verbindung mit Hilfe eines installierten Zertifikats. Es wird gemeldet, wenn beim Verbindungsversuch mit einem Server ein inkorrektes Zertifikat verwendet wird (wenn es z.B. von einem Angreifer ausgetauscht wurde).

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Link für die Anzeige des Zertifikats
- Mögliche Fehlerursachen
- Webadresse der Ressource

Folgende Aktionen stehen zur Auswahl:

- **Ja, unsicheres Zertifikat akzeptieren** – Verbindung mit der Webressource fortsetzen.
- **Zertifikat ablehnen** – Verbindung mit der Webressource trennen.

ERLAUBNISANFRAGE FÜR DEN ZUGRIFF AUF EINE WEBSEITE AUS EINER REGIONALEN DOMAIN

Wenn auf eine Webseite aus einer regionalen Domain zugegriffen wird, die nicht zu den verbotenen oder erlaubten Domains gehört, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung des Grunds, aus dem der Zugriff auf die Webseite blockiert wurde.
- Name der Region, zu der die Webseite gehört.
- Domain und Beschreibung des Kontaminationsgrads der Webseiten in dieser Domain
- Adresse der Webseite
- Name des Programms, das den Zugriff auf die Webseite ausgeführt hat.

Folgende Aktionen stehen zur Auswahl:

- **Ja, Zugriff erlauben** – Webseite laden.
- **Nein, Zugriff verbieten** – Laden der Webseite verwerfen.

Aktivieren Sie das Kontrollkästchen **Für diese Region speichern**, damit die gewählte Aktion auf alle Webseiten aus dieser regionalen Domain angewendet wird.

EIN PROGRAMM WURDE GEFUNDEN, DAS VON EINEM ANGREIFER BENUTZT WERDEN KANN, UM DEN COMPUTER ODER DIE BENUTZERDATEN ZU BESCHÄDIGEN

Wenn der Aktivitätsmonitor ein Programm erkennt, das von einem Angreifer benutzt werden kann, um den Computer oder die Benutzerdaten zu beschädigen, so erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Typ und Name des Programms, das von einem Angreifer benutzt werden kann, um den Computer oder die Benutzerdaten zu beschädigen

  Neben dem Namen des Programms befindet sich das Symbol ⓘ. Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über das Programm geöffnet.
- Prozess-ID, Name und Pfad der Programmdatei.
- Dieser Link führt zum Fenster mit einem Ereignisverlauf für das Programm.

Folgende Aktionen stehen zur Auswahl:

- **Erlauben** - Ausführen des Programms erlauben.
- **Quarantäne** – Programm beenden und Programmdatei in die Quarantäne verschieben, wo sie keine Gefahr für Ihren Computer darstellt.

  Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  > Der Status einer Datei, die in die Quarantäne verschoben wurde, kann sich bei einer erneuten Untersuchung in *virenfrei* ändern. Dies ist allerdings frühestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, möglich.
- **Programm beenden** – Ausführung des Programms abbrechen.
- **Zu Ausnahmen hinzufügen** – Dem Programm wird immer erlaubt, solche Aktionen auszuführen.

IN QUARANTÄNE BEFINDLICHE DATEI IST NICHT INFIZIERT

Kaspersky Internet Security untersucht die in Quarantäne befindlichen Dateien automatisch nach jedem Datenbankupdate. Wenn das Programm bei der Untersuchung einer in der Quarantäne befindlichen Datei feststellt, dass diese nicht infiziert ist, so erscheint eine entsprechende Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Empfehlung zur Wiederherstellung der in Quarantäne befindlichen Datei;
- Name der Datei, einschließlich des Pfades zum Ordner, in dem sich die Datei bis zu ihrer Verschiebung in die Quarantäne befand.

Folgende Aktionen stehen zur Auswahl:

- **Wiederherstellen** – Wiederherstellen der Datei durch Entfernen aus der Quarantäne und Ablegen in dem Ordner, in dem sie sich bis zum Verschieben in die Quarantäne befand.

- **Abbrechen** – das Objekt wird in der Quarantäne belassen.

EINE NEUE PRODUKTVERSION IST ERSCHIENEN

Wenn eine neue Version von Kaspersky Internet Security erschienen ist und zum Download auf den Kaspersky-Lab-Servern bereitsteht, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Link zum Fenster mit detaillierten Informationen über die erschienene Programmversion.
- Größe der Installationsdatei

Folgende Aktionen stehen zur Auswahl:

- **Ja, herunterladen** – Neue Programmversion in den festgelegten Ordner herunterladen.
- **Nein** – Download verwerfen.

Damit die Meldung über die neue Programmversion nicht mehr angezeigt wird, aktivieren Sie das Kontrollkästchen **Mich nicht über dieses Update informieren**.

EIN TECHNISCHES UPDATE IST ERSCHIENEN

Wenn ein technisches Update für Kaspersky Internet Security erschienen ist und zum Download auf den Kaspersky-Lab-Servern bereitsteht, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Versionsnummer des Programms, das auf dem Computer installiert ist.
- Versionsnummer des Programms nach dem angebotenen technischen Update
- Link zu einem Fenster mit ausführlichen Informationen zum technischen Update
- Größe der Updatedatei

Folgende Aktionen stehen zur Auswahl:

- **Ja, herunterladen** – Updatedatei in den festgelegten Ordner herunterladen.
- **Nein** – Download des Updates verwerfen. Diese Variante ist verfügbar, wenn das Kontrollkästchen **Mich nicht über dieses Update informieren** aktiviert ist (s. unten).
- **Nein, später erinnern** – Download des Updates jetzt verwerfen und später an das Update erinnern. Diese Variante ist verfügbar, wenn das Kontrollkästchen **Mich nicht über dieses Update informieren** deaktiviert ist (s. unten).

Aktivieren Sie das Kontrollkästchen **Mich nicht über dieses Update informieren**, damit die Meldung über dieses Update nicht mehr angezeigt wird.

EIN TECHNISCHES UPDATE WURDE HERUNTERGELADEN

Nachdem der Download eines technischen Updates für Kaspersky Internet Security abgeschlossen wurde, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Versionsnummer des Programms nach dem technischen Update

- Link zur Updatedatei

Folgende Aktionen stehen zur Auswahl:

- **Ja, installieren** – Update installieren.

  Nach der Installation des Updates kann ein Neustart des Betriebssystems erforderlich sein.

- **Installation aufschieben** – Installation verwerfen, um sie später auszuführen.

DAS HERUNTERGELADENE TECHNISCHE UPDATE WURDE NICHT INSTALLIERT

Wenn auf Ihrem Computer ein technisches Update für Kaspersky Internet Security vorhanden ist, das früher heruntergeladen wurde, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Versionsnummer des Programms nach dem technischen Update
- Link zur Updatedatei

Folgende Aktionen stehen zur Auswahl:

- **Ja, installieren** – Update installieren.

  Nach der Installation des Updates kann ein Neustart des Betriebssystems erforderlich sein.

- **Installation aufschieben** – Installation verwerfen, um sie später auszuführen.

Aktivieren Sie das Kontrollkästchen **Bis zum Erscheinen einer neuen Version nicht mehr fragen**, damit die Meldung über dieses Update nicht mehr angezeigt wird.

LIZENZ ABGELAUFEN

Bei Ablauf der Testlizenz zeigt Kaspersky Internet Security eine entsprechende Meldung auf dem Bildschirm an.

Die Meldung enthält folgende Informationen:

- Dauer des Testzeitraums;
- Informationen über die Ergebnisse der Programmausführung (kann einen Link zum Anzeigen ausführlicherer Daten beinhalten).

Folgende Aktionen stehen zur Auswahl:

- **Ja, kaufen** – bei Auswahl dieser Option öffnet sich der Browser und lädt die Seite des Webshops, wo Sie eine kommerzielle Lizenz für die Nutzung des Programms erwerben können.
- **Abbrechen** – Verzicht auf die Nutzung des Programms. Bei Auswahl dieser Variante stellt das Programm alle Hauptfunktionen ein (Virensuche, Echtzeitschutz-Funktionen usw.).

ES WIRD EMPFOHLEN, DIE DATENBANKEN VOR DER UNTERSUCHUNG ZU AKTUALISIEREN

Beim Start von Untersuchungsaufgaben wird vor oder während dem ersten Datenbank-Update eine Meldung angezeigt.

Dort wird empohlen, die Datenbanken zu aktualisieren oder den Abschluss des Updates abzuwarten, bevor eine Untersuchung ausgeführt wird.

Folgende Aktionen stehen zur Auswahl:

- **Datenbanken vor der Untersuchung aktualisieren** – Datenbank-Update starten. Nach dem Update wird automatisch die Untersuchungsaufgabe gestartet. Diese Variante ist verfügbar, wenn Sie eine Untersuchungsaufgabe gestartet haben, bevor die Datenbanken zum ersten Mal aktualisiert wurden.
- **Untersuchung nach dem Update starten** – Abschluss des Datenbank-Updates abwarten und Untersuchungsaufgabe automatisch starten. Diese Variante ist verfügbar, wenn Sie eine Untersuchungsaufgabe gestartet haben, während die Datenbanken zum ersten Mal aktualisiert werden.
- **Untersuchung jetzt starten** – Untersuchungsaufgabe starten, ohne ein Datenbank-Update abzuwarten.

MELDUNGEN IM INTERAKTIVEN SCHUTZMODUS

Dieser Abschnitt enthält alle Meldungen, die bei der Arbeit des Programms sowohl im automatischen als auch im interaktiven Schutzmodus erscheinen können (s. Abschnitt "Schutzmodus auswählen" auf S. 68).

IN DIESEM ABSCHNITT

NETZWERKAKTIVITÄT EINES PROGRAMMS WURDE ERKANNT

Wenn die Netzwerkaktivität eines Programms erkannt wird, erscheint auf dem Bildschirm eine Meldung (standardmäßig für Programme der Gruppen **Schwach beschränkt** oder **Stark beschränkt**).

Es wird eine Meldung angezeigt, wenn Kaspersky Internet Security im interaktiven Modus (s. Abschnitt "Schutzmodus auswählen" auf S. 68) arbeitet und für das Programm, dessen Netzwerkaktivität erkannt wurde, keine Paketregel (s. S. 117) erstellt wurde.

Die Meldung enthält folgende Informationen:

- Name des Programms und kurze Charakteristik der von ihm initiierten Verbindung.
- Informationen zur Verbindung (Verbindungstyp, lokaler Port und Remoteport, Adresse, mit der die Verbindung erfolgt).
- Startfolge eines Programms.

Folgende Aktionen stehen zur Auswahl:

- **Jetzt erlauben**.
- **Jetzt verbieten**.
- **Regel erstellen**. Bei Auswahl dieser Variante öffnet sich das Fenster **Firewall**, in dem Sie eine Regel erstellen können, mit der die Netzwerkaktivität des Programms reguliert wird (s. Abschnitt "Programmregeln ändern" auf S. 118).

Sie können die Netzwerkaktivität eines Programms einmalig oder für einen längeren Zeitraum verbieten oder erlauben. Wählen Sie dazu eine der folgenden Aktionen:

- **Jetzt erlauben** oder **Jetzt verbieten** – Netzwerkaktivität eines Programms ein Mal erlauben oder verbieten.
- **Jetzt erlauben** oder **Jetzt verbieten** (wenn das Kontrollkästchen **Speichern für diese Programmsitzung** aktiviert ist) – Ausgewählte Aktion für die gesamte Sitzung des Programms speichern, das eine Netzwerkaktivität gezeigt hat.

  Wenn in diesem Fenster das Kontrollkästchen **Speichern für immer** aktiviert ist, ändert sich durch Klick auf den Link **für immer** die Bezeichnung dieser Option in **Speichern für diese Programmsitzung**.
- **Jetzt erlauben** oder **Jetzt verbieten** (wenn das Kontrollkästchen **Speichern für immer** aktiviert ist) – Ausgewählte Aktion für immer speichern und immer anwenden.

  Wenn in diesem Fenster das Kontrollkästchen **Speichern für diese Programmsitzung** aktiviert ist, ändert sich durch Klick auf den Link **für diese Programmsitzung** die Bezeichnung dieser Option in **Speichern für immer**.

VERDÄCHTIGES / SCHÄDLICHES OBJEKT WURDE GEFUNDEN

Wenn von Datei-Anti-Virus oder Mail-Anti-Virus oder bei einer Virenuntersuchung eines der folgenden Objekte gefunden wird, erscheint eine Bildschirmmeldung:

- schädliches Objekt
- Objekt, das den Code eines unbekannten Virus enthält.
- Objekt, das den modifizierten Code eines bekannten Virus enthält.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Art der Bedrohung und Name des schädlichen Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines schädlichen Objekts befindet sich das Symbol ⓘ. Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung erhalten können, die dieses Objekt darstellt.
- Dateiname und Pfad eines schädlichen Objekts.

Sie können eine der folgenden Aktionen für das Objekt auswählen:

- **Desinfizieren** – Es wird versucht, das schädliche Objekt zu desinfizieren. Diese Variante wird vorgeschlagen, wenn es sich um eine bekannte Bedrohung handelt.

  Vor der Desinfektion wird eine Sicherungskopie des Objekts angelegt.
- **Quarantäne** – Objekt in die Quarantäne verschieben, wo es keine Gefahr für Ihren Computer darstellt. Diese Variante wird vorgeschlagen, wenn es sich um eine unbekannte Bedrohung handelt, für die bislang keine Desinfektionsmethoden vorliegen.

  Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  Der Status einer Datei, die in die Quarantäne verschoben wurde, kann sich bei einer erneuten Untersuchung in *virenfrei* ändern. Dies ist allerdings frühestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, möglich.
- **Löschen** – Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt.
- **Überspringen / Blockieren** – Zugriff auf das Objekt sperren. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

Damit die gewählte Aktion auf alle Bedrohungen dieses Typs angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder der Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente, die vom Start bis zum Beenden einer Komponente oder bis zum Neustart von Kaspersky Internet Security dauert, sowie die Ausführungszeit einer Untersuchungsaufgabe vom Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Objekt ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass das Programm bei der Arbeit mit diesem Objekt erneut anspricht.

EINE SCHWACHSTELLE WURDE GEFUNDEN

Beim Fund einer Schwachstelle erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Schwachstelle
- Name der Schwachstelle gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen befindet sich das Symbol ⓘ. Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über die Schwachstelle geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Schwachstelle erhalten können.

- Dateiname und Pfad des anfälligen Objekts.

Sie können eine der folgenden Aktionen für das Objekt auswählen:

- **Ja, korrigieren** – Schwachstelle beheben.
- **Überspringen** – Keine Aktionen mit dem anfälligen Objekt ausführen.

ANFRAGE AUF ERLAUBNIS FÜR PROGRAMMAKTIONEN

Wenn ein Programm versucht, eine Aktion auszuführen, über deren Sicherheit oder Notwendigkeit Kaspersky Internet Security keine Informationen vorliegen, so erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Name und Symbol ⓘ des Programms Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über das Programm geöffnet.
- Beschreibung der Programmaktionen
- Ort der Programmdatei
- Startfolge des Programms

Sie können die Ausführung des Programms erlauben oder verbieten. Wählen Sie dazu eine der folgenden Aktionen:

- **Vertrauenswürdig machen** – Programm in die Gruppe *Vertrauenswürdig* verschieben (Die Ausführung des Programms wird immer erlaubt).
- **Jetzt erlauben** – Ausführung des Programms einmal erlauben.
- **Jetzt verbieten** – Ausführung des Programms einmal verbieten.
- **Programm beenden und als nicht vertrauenswürdig einstufen** – Programm in die Gruppe *Nicht vertrauenswürdig* verschieben (Die Ausführung des Programms wird immer verboten).

GEFÄHRLICHE AKTIVITÄT IM SYSTEM WURDE ERKANNT

Wenn der Proaktive Schutz die gefährliche Aktivität einer bestimmten Anwendung im System erkennt, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung

- Art der Bedrohung und Name des schädlichen Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines schädlichen Objekts befindet sich das Symbol ⓘ. Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung erhalten können, die dieses Objekt darstellt.

- Prozess-ID, Name und Pfad der Programmdatei.

Folgende Aktionen stehen zur Auswahl:

- **Erlauben** - Ausführen des Programms erlauben.
- **Quarantäne** – Programm beenden und Programmdatei in die Quarantäne verschieben, wo sie keine Gefahr für Ihren Computer darstellt.

  Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  Der Status einer Datei, die in die Quarantäne verschoben wurde, kann sich bei einer erneuten Untersuchung in *virenfrei* ändern. Dies ist allerdings frühestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, möglich.

- **Programm beenden** – Ausführung des Programms abbrechen.
- **Zu Ausnahmen hinzufügen** – Dem Programm wird immer erlaubt, solche Aktionen auszuführen.

Wenn Sie überzeugt sind, dass das gefundene Programm ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass Kaspersky Internet Security erneut anspricht, wenn er das Programm findet.

ROLLBACK VON ÄNDERUNGEN, DIE VON EINEM PROGRAMM AUSGEFÜHRT WURDEN, DAS VON EINEM ANGREIFER BENUTZT WERDEN KANN, UM DEN COMPUTER ODER DIE BENUTZERDATEN ZU BESCHÄDIGEN.

Es wird empfohlen, Änderungen, die von einem Programm ausgeführt wurden, das von einem Angreifer benutzt werden kann, um den Computer oder die Benutzerdaten zu beschädigen, rückgängig zu machen (zu verwerfen). Wenn dieses Programm beendet wird, erscheint auf dem Bildschirm eine Anfrage zum Rollback der Veränderungen.

Die Meldung enthält folgende Informationen:

- Anfrage auf ein Rollback von Veränderungen, die das Programm, das von einem Angreifer benutzt werden kann, um den Computer oder die Benutzerdaten zu beschädigen, ausgeführt hat.
- Typ und Name des Programms

  Neben dem Namen des Programms befindet sich das Symbol ⓘ. Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über das Programm geöffnet.

- Prozess-ID, Name und Pfad der Programmdatei.

Folgende Aktionen stehen zur Auswahl:

- **Überspringen** – Veränderungen nicht rückgängig machen.
- **Ja, rückgängig machen** – Veränderungen rückgängig machen, die von diesem Programm ausgeführt wurden.

EIN SCHÄDLICHES PROGRAMM WURDE GEFUNDEN

Wenn der Aktivitätsmonitor ein Programm erkennt, dessen Verhalten mit den Aktionen von Schadprogrammen übereinstimmt, wird dies gemeldet.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Typ und Name des schädlichen Programms

  Neben dem Namen des Programms befindet sich das Symbol ⓘ. Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über das Programm geöffnet.

- Prozess-ID, Name und Pfad der Programmdatei.
- Dieser Link führt zum Fenster mit einem Ereignisverlauf für das Programm.

Folgende Aktionen stehen zur Auswahl:

- **Erlauben** - Ausführen des Programms erlauben.
- **Quarantäne** – Programm beenden und Programmdatei in die Quarantäne verschieben, wo sie keine Gefahr für Ihren Computer darstellt.

  Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  Der Status einer Datei, die in die Quarantäne verschoben wurde, kann sich bei einer erneuten Untersuchung in *virenfrei* ändern. Dies ist allerdings frühestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, möglich.

- **Programm beenden** – Ausführung des Programms abbrechen.
- **Zu Ausnahmen hinzufügen** – Dem Programm wird immer erlaubt, solche Aktionen auszuführen.

EIN PROGRAMM, DAS VON ANGREIFERN VERWENDET WERDEN KANN, WURDE GEFUNDEN

Wenn von Datei-Anti-Virus, Mail-Anti-Virus oder von einer Untersuchungsaufgabe ein Programm gefunden wird, das von Angreifern verwendet werden kann, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Art der Bedrohung und Name des Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines Objekts befindet sich das Symbol ⓘ. Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Seite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen erhalten können.

- Dateiname und Pfad des Objekts.

Sie können eine der folgenden Aktionen für das Objekt auswählen:

- **Quarantäne** – Objekt in die Quarantäne verschieben, wo es keine Gefahr für Ihren Computer darstellt. Diese Variante wird vorgeschlagen, wenn es sich um eine unbekannte Bedrohung handelt, für die bislang keine Desinfektionsmethoden vorliegen.

  Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  Der Status einer Datei, die in die Quarantäne verschoben wurde, kann sich bei einer erneuten Untersuchung in *virenfrei* ändern. Dies ist allerdings frühestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, möglich.

- **Löschen** – Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt.
- **Archiv löschen** – Kennwortgeschütztes Archiv löschen.
- **Überspringen / Blockieren** – Zugriff auf das Objekt sperren. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

- **Zu Ausnahmen hinzufügen** – Ausnahmeregel für diesen Bedrohungstyp erstellen.

Damit die gewählte Aktion auf alle Bedrohungen dieses Typs angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder der Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente, die vom Start bis zum Beenden einer Komponente oder bis zum Neustart von Kaspersky Internet Security dauert, sowie die Ausführungszeit einer Untersuchungsaufgabe vom Start bis zum Abschluss.

Wenn Sie überzeugt sind, dass das gefundene Objekt ungefährlich ist, können Sie es der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass das Programm bei der Arbeit mit diesem Objekt erneut anspricht.

EIN VERDÄCHTIGER / SCHÄDLICHER LINK WURDE GEFUNDEN

Wenn Kaspersky Internet Security erkennt, dass versucht wird, eine Webseite mit schädlichem oder verdächtigem Inhalt zu öffnen, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Name des Programms (Browsers), mit dem das Laden der Webseite ausgeführt wird.
- Adresse der Website oder Webseite mit schädlichem oder verdächtigem Inhalt.

Folgende Aktionen stehen zur Auswahl:

- **Erlauben** – Download der Webseite fortsetzen.
- **Verbieten** – Download der Webseite blockieren.

Damit die gewählte Aktion auf alle Webseiten angewendet wird, die eine Bedrohung dieses Typs enthalten und die während der laufenden Sitzung der Schutzkomponente gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente. Diese dauert vom Start bis zum Beenden einer Komponente oder bis zum Neustart von Kaspersky Internet Security.

GEFÄHRLICHES OBJEKT WURDE IM DATENSTROM GEFUNDEN

Wenn Web-Anti-Virus im Datenverkehr ein gefährliches Objekt findet, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung oder der Aktionen, die ein Programm ausführen kann.
- Name des Programms, das eine Aktion ausführt.
- Art der Bedrohung und Name des schädlichen Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines schädlichen Objekts befindet sich das Symbol . Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung erhalten können, die dieses Objekt darstellt.
- Ort des Objekts (URL-Adresse).

Folgende Aktionen stehen zur Auswahl:

- **Erlauben**- Download des Objekts fortsetzen.
- **Verbieten** – Download des Objekts von der Webressource blockieren.

Damit die gewählte Aktion auf alle Bedrohungen dieses Typs angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder der Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente. Diese dauert vom Start bis zum Beenden einer Komponente oder bis zum Neustart von Kaspersky Internet Security.

EIN VERSUCHTER ZUGRIFF AUF EINE PHISHING-SEITE WURDE ERKANNT

Wenn Kaspersky Internet Security erkennt, dass versucht wird, auf eine Webseite zuzugreifen, die als Phishing-Seite bekannt ist oder des Phishings verdächtig ist, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Adresse der Webseite

Folgende Aktionen stehen zur Auswahl:

- **Erlauben** – Download der Webseite fortsetzen.
- **Verbieten** – Download der Webseite blockieren.

Damit die gewählte Aktion auf alle Webseiten angewendet wird, die eine Bedrohung dieses Typs enthalten und die während der laufenden Sitzung von Kaspersky Internet Security gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente. Diese dauert vom Start bis zum Beenden einer Komponente oder bis zum Neustart von Kaspersky Internet Security.

VERSUCH ZUM ZUGRIFF AUF DIE SYSTEMREGISTRIERUNG WURDE ERKANNT

Wenn der Proaktive Schutz erkennt, dass versucht wird, Zugriff auf Schlüssel der Systemregistrierung zu erhalten, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Registrierungsschlüssel, auf den versucht wurde, Zugriff zu erhalten.
- Dateiname und Pfad des Prozesses, der versucht hat, Zugriff auf Registrierungsschlüssel zu erhalten.

Folgende Aktionen stehen zur Auswahl:

- **Erlauben** - Das Ausführen der gefährlichen Aktion einmal erlauben.
- **Verbieten** - Das Ausführen der gefährlichen Aktion einmal verbieten.

Damit die von Ihnen gewählte Aktion jedes Mal ausgeführt wird, wenn versucht wird, Zugriff auf Registrierungsschlüssel zu erhalten, aktivieren Sie das Kontrollkästchen **Regel erstellen**.

Wenn Sie überzeugt sind, dass jede Aktivität der Anwendung, die den Zugriff auf die Systemregistrierungsschlüssel initiierte, ungefährlich ist, fügen Sie diese Anwendung der Liste der vertrauenswürdigen Anwendungen hinzu.

DESINFEKTION DES OBJEKTS IST NICHT MÖGLICH

Es kann vorkommen, dass sich ein Objekt nicht desinfizieren lässt (beispielsweise weil eine Datei so stark beschädigt ist, dass der schädliche Code nicht daraus gelöscht und sie vollständig wiederhergestellt werden kann). Der Desinfektionsvorgang ist auf einige Arten von schädlichen Objekten nicht anwendbar, beispielsweise auf Trojaner-Programme. Wenn die Desinfektion eines Objekts nicht möglich ist, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Art der Bedrohung und Name des schädlichen Objekts gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen eines schädlichen Objekts befindet sich das Symbol ⓘ. Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über das Objekt geöffnet. Aus diesem Fenster gelangen Sie über den Link www.securelist.com zur Webseite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung erhalten können, die dieses Objekt darstellt.

- Dateiname und Pfad eines schädlichen Objekts.

Folgende Aktionen stehen zur Auswahl:

- **Löschen** – Objekt löschen. Vor dem Löschen wird eine Sicherungskopie des Objekts angelegt.
- **Überspringen / Blockieren** – Zugriff auf das Objekt sperren. Keine Aktion mit dem Objekt vornehmen, sondern nur Informationen darüber im Bericht aufzeichnen.

  Sie können später aus dem Berichtsfenster zur Verarbeitung von übersprungenen schädlichen Objekten zurückkehren (für Objekte, die in E-Mails gefunden wurden, steht die Option zur aufgeschobenen Verarbeitung nicht zur Verfügung).

- **Zu Ausnahmen hinzufügen** – Ausnahmeregel für diesen Bedrohungstyp erstellen.

Damit die gewählte Aktion auf alle Bedrohungen dieses Typs angewendet wird, die während der laufenden Sitzung der Schutzkomponente oder der Aufgabe gefunden werden, aktivieren Sie das Kontrollkästchen **Auf alle Objekte anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente, die vom Start bis zum Beenden einer

Komponente oder bis zum Neustart von Kaspersky Internet Security dauert, sowie die Ausführungszeit einer Untersuchungsaufgabe vom Start bis zum Abschluss.

VERSTECKTER PROZESS WURDE GEFUNDEN

Wenn der Proaktive Schutz einen versteckten Prozess im System findet, erscheint eine Meldung auf dem Bildschirm.

Die Meldung enthält folgende Informationen:

- Beschreibung der Bedrohung
- Art und Name der Bedrohung gemäß der Viren-Enzyklopädie von Kaspersky Lab.

  Neben dem Namen befindet sich das Symbol . Durch Klick auf dieses Symbol wird ein Fenster mit Informationen über die Bedrohung geöffnet. Aus diesem Fenster gelangen Sie über den Link www.viruslist.com/de zur Seite der Viren-Enzyklopädie, auf der Sie ausführliche Informationen über die Bedrohung finden.
- Name und Pfad der Prozessdatei

Folgende Aktionen stehen zur Auswahl:

- **Quarantäne** – Prozess beenden und Prozessdatei in die Quarantäne verschieben, wo sie keine Gefahr für Ihren Computer darstellt.

  Bei späteren Untersuchungen der Quarantäne kann sich der Status eines Objekts ändern. Das Objekt kann beispielsweise als infiziert erkannt und mit Hilfe aktualisierter Datenbanken verarbeitet werden, oder es erhält den Status *virenfrei* und kann dann wiederhergestellt werden.

  Der Status einer Datei, die in die Quarantäne verschoben wurde, kann sich bei einer erneuten Untersuchung in *virenfrei* ändern. Dies ist allerdings frühestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, möglich.
- **Beenden** – Prozess abbrechen.
- **Erlauben** - Das Ausführen des Prozesses erlauben.

Damit die gewählte Aktion auf alle Bedrohungen dieses Typs angewendet wird, die während der laufenden Sitzung des Proaktiven Schutzes gefunden werden, aktivieren Sie das Kontrollkästchen **In allen ähnlichen Fällen anwenden**. Als laufende Sitzung gilt die Arbeitszeit einer Komponente. Diese dauert vom Start bis zum Beenden einer Komponente oder bis zum Neustart von Kaspersky Internet Security.

Wenn Sie überzeugt sind, dass der gefundene Prozess ungefährlich ist, können Sie ihn der vertrauenswürdigen Zone hinzufügen, um zu verhindern, dass Kaspersky Internet Security erneut anspricht, wenn er den Prozess findet.

VERBOTENE REGION DER DOMAIN / ZUGRIFF VERBOTEN

Web-Anti-Virus kann den Zugriff auf eine Webseite auf Basis ihrer Zugehörigkeit zu einer regionalen Domain blockieren. Eine Domain gilt in folgenden Fällen als verboten:

- Zugriff auf die Domain wurde vom Benutzer bei der Konfiguration von Web-Anti-Virus verboten.
- Ein vorhergehender Zugriff auf eine Webseite aus dieser Region wurde vom Benutzer verboten.

Wenn der Geo-Filter (Modul von Web-Anti-Virus) erkennt, dass versucht wird, eine Webseite zu öffnen, die einer verbotenen Region angehört, erscheint eine Meldung im Browserfenster.

Die Meldung enthält folgende Informationen:

- Beschreibung des Grunds, aus dem der Zugriff auf die Webseite blockiert wurde.
- Name der Region, zu der die Webseite gehört.
- Domain und Beschreibung des Kontaminationsgrads der Webseiten in dieser Domain
- URL-Adresse der Webseite.

Folgende Aktionen stehen zur Auswahl:

- **Zur vorherigen Seite zurückkehren** – Vorherige Webseite öffnen.
- **Webressource öffnen** – Webseite, die zu einer verbotenen Domain gehört, laden.
- **Einstellungen für Geo-Filter öffnen** – Konfigurationsfenster für Web-Anti-Virus auf der Registerkarte **Geo-Filter** öffnen.

GEFÄHRLICHE WEBRESSOURCE

Wenn der Web-Filter (Modul von Web-Anti-Virus) erkennt, dass versucht wird, eine gefährliche Webseite zu öffnen, erscheint eine Meldung im Browserfenster.

Die Meldung enthält folgende Informationen:

- Beschreibung des Grunds, aus dem der Zugriff auf die Webseite blockiert wurde.
- Adresse der Webseite

Folgende Aktionen stehen zur Auswahl:

- **Zur vorherigen Seite zurückkehren** – Gefährliche Webseite nicht laden und vorherige Seite öffnen.
- **In jedem Fall öffnen** – Gefährliche Webseite laden.

KEINE DATEN ZUR SICHERHEIT DER WEBRESSOURCE VORHANDEN

Wenn der Web-Filter (Modul von Web-Anti-Virus) erkennt, dass versucht wird, eine Webseite zu öffnen, über die keine zuverlässigen Sicherheitsdaten vorliegen, so erscheint eine Meldung im Browserfenster.

Die Meldung enthält folgende Informationen:

- Beschreibung des Grunds, aus dem der Zugriff auf die Webseite angehalten wurde.
- Adresse der Webseite

Folgende Aktionen stehen zur Auswahl:

- **Ja, Webressource öffnen** – Webseite laden.
- **Öffnen und zu vertrauenswürdigen Adressen hinzufügen** – Webseite laden und ihre Adresse zur vertrauenswürdigen Liste hinzufügen, damit der Web-Filter das Laden dieser Webseite künftig nicht mehr anhält.
- **Im Sicheren Browser öffnen** – Webseite im Sicheren Browser laden (nur für die Browser Microsoft Internet Explorer, Mozilla Firefox und Google Chrome). Wenn schädliche Objekte, die sich auf zu ladenden Seiten befinden, im Sicheren Browser geladen werden, stellen sie keine Gefahr für die Computersicherheit dar.

- **Nein, zur vorherigen Seite zurückkehren** – Webseite nicht laden und vorherige Seite öffnen.

ES WIRD EMPFOHLEN, IN DEN MODUS FÜR DEN SICHEREN BROWSER ZU WECHSELN.

Für das Online-Banking empfiehlt Kaspersky Lab den Einsatz des Modus für den Sicheren Browser, der Ihren persönlichen Daten erhöhte Sicherheit bietet.

Wenn versucht wird, eine Webseite für Online-Banking zu öffnen, zeigt Web-Anti-Virus im Browserfenster eine Meldung an.

Die Meldung enthält folgende Informationen:

- Empfehlung, in den Modus für den Sicheren Browser zu wechseln.
- Adresse der Ressource für Online-Banking.

Folgende Aktionen stehen zur Auswahl:

- **Im Modus "Sicherer Browser" öffnen** – Webseite unter Verwendung des Sicheren Browsers öffnen (nur für die Browser Microsoft Internet Explorer, Mozilla Firefox und Google Chrome).
- **Webseite öffnen** – Webseite im normalen Modus öffnen.
- **Zur vorherigen Seite zurückkehren** – Webseite nicht öffnen und vorherige Seite im normalen Modus öffnen.

ES WIRD EMPFOHLEN, DEN MODUS FÜR DEN SICHEREN BROWSER ZU VERLASSEN.

Bei der Arbeit mit Online-Banking-Seiten wird der Modus für den Sicheren Browser verwendet. Wenn Sie auf eine andere Webseite wechseln, die nichts mit Online-Banking zu tun hat, wird empfohlen, den Sicheren Browsermodus zu verlassen. Wenn Sie mit einer gewöhnlichen Webseite im Sicheren Browsermodus weiterarbeiten, kann dies den Schutz Ihrer persönlichen Daten beeinträchtigen.

Wenn im Modus für den Sicheren Browser versucht wird, von einer Webseite für Online-Banking auf eine andere Webseite zu wechseln, zeigt Web-Anti-Virus im Browserfenster eine Meldung an.

Die Meldung enthält folgende Informationen:

- Empfehlung, den Modus für den Sicheren Browser zu verlassen.
- Adresse der Webseite, auf die Sie von der Online-Banking-Seite aus wechseln möchten.

Folgende Aktionen stehen zur Auswahl:

- **Webressource im normalen Browser öffnen** – Sicheren Browsermodus beenden und Webseite im normalen Modus öffnen.
- **Das ist eine Banking-Webseite. Im Modus "Sicherer Browser" fortsetzen** – Im Sicheren Browser bleiben und Webseite öffnen.
- **Zur vorherigen Seite zurückkehren** – Vorherige Webseite im Sicheren Browsermodus öffnen.

GLOSSAR

2

2-Channel-Gateway

Computer mit zwei Netzwerkadaptern, die an verschiedene Netzwerke angeschlossen sind und Daten von einem Netzwerk an ein anderes Netzwerk übermitteln.

A

Aktive Lizenz

Lizenz, die momentan für die Arbeit des Kaspersky-Lab-Programms verwendet wird. Die Lizenz legt die Gültigkeitsdauer für den vollen Funktionsumfang sowie die Lizenzpolitik für das Programm fest. Im Programm kann nur ein Schlüssel den Status "aktiv" besitzen.

Alternative NTFS-Datenströme

Datenströme des NTFS-Dateisystems (alternate data streams), die für zusätzliche Attribute oder Datei-Informationen vorgesehen sind.

Jede Datei im NTFS-Dateisystem stellt eine Auswahl von Datenströmen (streams) dar. In einem Datenstrom befindet sich der Datei-Inhalt, den man sehen kann, wenn man die Datei öffnet, die übrigen (alternativen) Datenströme sind für Meta-Informationen vorgesehen und bieten zum Beispiel die Kompatibilität des NTFS-Systems mit anderen Systemen, wie mit dem alten Dateisystem von Macintosh - Hierarchical File System (HFS). Die Datenströme lassen sich erstellen, löschen, separat speichern, umbenennen und sogar als Prozess starten.

Alternative Datenströme können von Angreifern missbraucht werden, um Daten des Computers heimlich zu übertragen oder zu empfangen.

Anstößige E-Mail

Nachricht, die anstößige Ausdrücke enthält.

Archiv

Datei, die ein oder mehrere Objekte "enthält", die ihrerseits auch Archive sein können.

Aufgabe

Funktionen, die das Kaspersky-Lab-Programm ausführen kann und die als Aufgaben realisiert sind, Beispiele: Echtzeitschutz für Dateien, Vollständige Untersuchung des Computers, Datenbank-Update.

Aufgabeneinstellungen

Parameter für die Arbeit des Programms, die für jeden Aufgabentyp individuell sind.

Ausnahme

Eine Ausnahme ist ein Objekt, das von der Untersuchung durch das Kaspersky-Lab-Programm ausgeschlossen wird. Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm) sowie Programmprozesse oder Objekte nach einem Bedrohungstyp gemäß der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden. Für jede Aufgabe können individuelle Ausnahmen festgelegt werden.

Autostart-Objekte

Auswahl von Programmen, die für den Start und die korrekte Funktion des auf Ihrem Computer installierten Betriebssystems und der vorhandenen Software erforderlich sind. Diese Objekte werden jedes Mal beim Hochfahren des Betriebssystems gestartet. Es gibt Viren, die speziell diese Objekte infizieren können. Dadurch kann beispielsweise das Hochfahren des Betriebssystems blockiert werden.

B

BENACHRICHTIGUNGSVORLAGE

Vorlage, mit der bei der Untersuchung erkannte infizierte Objekte gemeldet werden. Eine Benachrichtigungsvorlage enthält mehrere Einstellungen, die die Reihenfolge der Benachrichtigung, die Verbreitungsart und den Meldungstext definieren.

BOOTVIRUS

Virus, der die Bootsektoren von Computerlaufwerken infiziert. Der Virus "zwingt" das System beim Hochfahren, nicht auf den eigentlichen Bootcode zuzugreifen, sondern auf den Viruscode, der dann die Kontrolle übernimmt.

D

DATEIMASKE

Platzhalter für den Namen und die Erweiterung einer Datei, der aus allgemeinen Zeichen besteht. Die zwei wichtigsten Zeichen, die in Dateimasken verwendet werden sind * und ? (wobei * für eine beliebige Anzahl von beliebigen Zeichen und ? für ein beliebiges Einzelzeichen steht). Mit Hilfe dieser Zeichen kann jede beliebige Datei dargestellt werden. Beachten Sie, dass Name und Endung einer Datei stets durch einen Punkt getrennt werden.

DATENBANK FÜR PHISHING-WEBADRESSEN

Eine Liste der Webressourcen, die von den Kaspersky-Lab-Spezialisten als Phishing-Adressen eingestuft wurden. Die Datenbank wird regelmäßig aktualisiert und gehört zum Lieferumfang des Kaspersky-Lab-Programms.

DATENBANK FÜR VERDÄCHTIGE WEBADRESSEN

Eine Liste der Webressourcen, deren Inhalt als potenziell gefährlich eingestuft werden kann. Die Liste ist von den Kaspersky-Lab-Spezialisten angelegt, wird regelmäßig aktualisiert und gehört zum Lieferumfang des Programms.

DATENBANK-UPDATE

Eine Funktion, die vom Kaspersky-Lab-Programm ausgeführt wird und die es erlaubt, den aktuellen Zustand des Schutzes aufrecht zu erhalten. Dabei werden die Datenbanken von den Kaspersky-Lab-Updateservern auf den Computer kopiert und automatisch von der Anwendung übernommen.

DATENBANKEN

Datenbanken, die von den Kaspersky-Lab-Spezialisten gepflegt werden und eine genaue Beschreibung aller momentan existierenden Bedrohungen der Computersicherheit sowie Methoden zu ihrer Identifikation und Desinfektion enthalten. Die Datenbanken werden von Kaspersky Lab laufend aktualisiert, wenn neue Bedrohungen auftauchen.

DESINFEKTION VON OBJEKTEN

Methode zur Bearbeitung von infizierten Objekten, bei der die Daten vollständig oder teilweise wiederhergestellt werden oder eine Entscheidung darüber getroffen wird, dass die Desinfektion von Objekten nicht möglich ist. Die Desinfektion von Objekten erfolgt auf Basis der Einträge in den Datenbänken. Bei der Desinfektion können Daten teilweise verloren gehen.

DESINFEKTION VON OBJEKTEN BEIM NEUSTART

Methode zur Verarbeitung von infizierten Objekten, die im Augenblick der Desinfektion von anderen Programmen verwendet werden. Dabei wird eine Kopie des infizierten Objekts angelegt. Beim folgenden Neustart wird die Kopie desinfiziert und das infizierte Originalobjekt wird durch die desinfizierte Kopie ersetzt.

DOMAIN NAME SERVICE (DNS)

Verbreitetes System zur Umformung von Hostnamen (Computer oder anderes Netzwerkgerät) in eine IP-Adresse. DNS funktioniert in TCP/IP-Netzwerken. Im Einzelfall kann DNS auch umgekehrte Anfragen und Definitionen von Hostnamen nach dessen IP (PTR-Eintrag) speichern und verarbeiten. Die Auflösung von DNS-Namen erfolgt gewöhnlich durch Netzwerkprogramme und nicht durch die Benutzer.

DRINGENDES UPDATE

Kritisches Update für die Module des Kaspersky-Lab-Programms.

E

E-MAIL LÖSCHEN

Verarbeitungsmethode für eine E-Mail, bei der die Nachricht physikalisch gelöscht wird. Diese Methode wird für E-Mails empfohlen, die eindeutig Spam oder ein schädliches Objekt enthalten. Vor dem Löschen einer Nachricht, wird ihre Kopie im Backup gespeichert (wenn diese Funktion nicht deaktiviert wurde).

ECHTZEITSCHUTZ

Funktionsmodus des Programms, in dem Objekte im Echtzeitmodus auf schädlichen Code untersucht werden.

Das Programm fängt jeden Versuch zum Öffnen, Schreiben und Ausführen eines Objekts ab, und durchsucht das Objekt nach Bedrohungen. Virenfreie Objekte werden für den Zugriff freigegeben, infizierte oder verdächtige Objekte werden gemäß den Aufgabenparametern verarbeitet (desinfiziert, gelöscht, in die Quarantäne verschoben).

EIN- UND AUSGABEPORT

Wird in Mikroprozessoren (z.B. Intel) beim Datenaustausch mit der Hardware verwendet. Der Ein- und Ausgabeport wird einem bestimmten Gerät zugeordnet und erlaubt es den Programmen, zum Datenaustausch darauf zuzugreifen.

EMPFOHLENE STUFE

Sicherheitsstufe, deren Funktionsparameter von Kaspersky Lab empfohlen werden und die einen optimalen Schutz Ihres Computers gewährleistet. Diese Stufe wird in der Grundeinstellung verwendet.

F

FEHLALARM

Situation, in der ein virenfreies Objekt von der Kaspersky-Lab-Anwendung als infiziert eingestuft wird, weil sein Code Ähnlichkeit mit einem Virus aufweist.

G

GEFÄHRLICHES OBJEKT

Objekt, in dem sich ein Virus befindet. Es wird davor gewarnt, mit solchen Objekten zu arbeiten, weil dies zur Infektion des Computers führen kann. Beim Fund eines infizierten Objekts wird empfohlen, das Objekt mit Hilfe eines Kaspersky-Lab-Programms zu desinfizieren oder, falls die Desinfektion nicht möglich ist, es zu löschen.

GEPACKTE DATEI

Archivdatei, die ein Extrahierprogramm und für das Betriebssystem bestimmte Extrahierbefehle enthält.

GÜLTIGKEITSDAUER DER LIZENZ

Zeitraum, für den Sie berechtigt sind, das Kaspersky-Lab-Programm mit allen Funktionen zu nutzen. Die Gültigkeitsdauer der Lizenz beträgt in der Regel ein Kalenderjahr ab der Installation der Lizenz. Wenn die Gültigkeitsdauer der Lizenz abgelaufen ist, wird die Funktionalität des Programms eingeschränkt: Das Update der Datenbanken ist nicht mehr verfügbar.

H

HARDWARE-PORT

Eingang an einem Hardware-Element des Computers, an den ein Kabel oder ein Stecker angeschlossen werden kann (LPT-Port, serieller Port, USB).

HEURISTISCHE ANALYSE

Technologie zum Erkennen von Bedrohungen, die nicht mit Hilfe der Datenbanken für Kaspersky-Lab-Programme identifiziert werden können. Es wird erlaubt, Objekte zu finden, die verdächtig sind, durch einen unbekannten Virus oder eine neue Modifikation eines bekannten Virus infizierte zu sein.

Mit Hilfe der heuristischen Analyse werden bis zu 92 % der neuen Bedrohungen erkannt. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Dateien, die mit Hilfe der heuristischen Analyse gefunden werden, nennt man verdächtig.

I

ICHECKER-TECHNOLOGIE

Diese Technologie erlaubt eine Erhöhung der Untersuchungsgeschwindigkeit. Dabei werden jene Objekte von der Untersuchung ausgeschlossen, die seit dem vorherigen Scannen nicht verändert wurden, wobei vorausgesetzt wird, dass die Untersuchungsparameter (Antiviren-Datenbanken und Einstellungen) gleich geblieben sind. Informationen darüber werden einer speziellen Datenbank aufgezeichnet. Die Technologie wird sowohl für den Echtzeitschutz als auch für den Scan auf Befehl verwendet.

Wurde beispielsweise eine Archivdatei vom Programm untersucht und ihr wurde der Status virenfrei zugewiesen. Dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn seit der letzten Untersuchung die Zusammensetzung des Archivs durch Hinzufügen eines neuen Objekts verändert wurde, die Untersuchungsparameter geändert oder die Programm-Datenbanken aktualisiert wurden, wird das Archiv erneut untersucht.

Einschränkungen der Technologie iChecker:

Die Technologie funktioniert nicht mit großen Dateien, da die Untersuchung der gesamten Datei in diesem Fall weniger Zeit beansprucht, als zu ermitteln, ob sie seit der letzten Untersuchung verändert wurde.

Die Technologie unterstützt eine begrenzte Anzahl von Formaten (exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

INDIKATOR FÜR EINE VIRENEPIDEMIE

Vorlage, auf der eine Benachrichtigung über den drohenden Ausbruch einer Virenepidemie beruht. Der Indikator für eine Virenepidemie umfasst einige Einstellungen, die den Schwellenwert der Virenaktivität, die Verbreitungsart und den Meldungstext enthalten.

INFIZIERTES OBJEKT

Objekt, das schädlichen Code enthält: Bei der Untersuchung des Objekts wurde erkannt, dass ein Abschnitt des Objektcodes vollständig mit dem Code einer bekannten Bedrohung übereinstimmt. Die Kaspersky-Lab-Spezialisten warnen davor, mit solchen Objekten zu arbeiten, da dies zur Infektion Ihres Computers führen kann.

INKOMPATIBLES PROGRAMM

Antiviren-Programm eines Drittherstellers oder Kaspersky-Lab-Programm, das nicht mit Kaspersky Internet Security verwaltet werden kann.

INSTALLATION MIT LOGIN-SZENARIO

Remote-Installation von Kaspersky-Lab-Programmen, mit der der Start der Aufgabe zur Remote-Installation mit einem konkreten Benutzerkonto (mehreren Benutzerkonten) verknüpft werden kann. Beim Anmelden des Benutzers in der Domäne wird versucht, das Programm auf dem Client-Computer zu installieren, auf dem sich der Benutzer angemeldet hat. Dieses Verfahren wird für die Installation von Programmen des Herstellers auf Computern mit den Betriebssystemen Microsoft Windows 98 / Me empfohlen.

INTERCEPTOR

Subkomponente des Programms, die für die Untersuchung bestimmter Typen von E-Mails verantwortlich ist. Die Auswahl der zu installierenden Interceptoren ist davon abhängig, in welcher Rolle oder Rollenkombination das Programm eingesetzt werden soll.

INTERNETPROTOKOLL (IP)

Basisprotokoll für das Internet, das seit seiner Entwicklung im Jahre 1974 unverändert verwendet wird. Es führt die Grundoperationen bei der Datenübertragung von einem Computer auf einen anderen aus und dient als Basis für alle Protokolle höherer Ebenen wie TCP und UDP. Es kontrolliert die Verbindung und die Fehlerbehandlung. Technologien wie NAT und Masquerading ermöglichen es, umfangreiche Netzwerke hinter einer relativ geringen Anzahl von IP-Adressen zu verbergen (oder sogar hinter einer Adresse). Dadurch wird erlaubt, die Ansprüche des ständig expandierenden Internets unter Verwendung eines relativ begrenzten IPv4-Adressraums zu befriedigen.

K

KASPERSKY SECURITY NETWORK

Kaspersky Security Network (KSN) ist eine Infrastruktur der Online-Dienste und -Services, die den Zugriff auf die aktuelle Wissensdatenbank von Kaspersky Lab über den "Ruf" der Dateien, Internet-Ressourcen und Programme bietet. Durch die Verwendung der Daten von Kaspersky Security Network wird die Geschwindigkeit der Reaktion von Kaspersky Internet Security auf neue Bedrohungen und die Leistungsfähigkeit einiger Komponenten erhöht. Außerdem wird dadurch das Risiko verringert, dass Fehlalarme auftreten.

KASPERSKY-LAB-UPDATESERVER

Liste der HTTP- und FTP-Server von Kaspersky Lab, von denen das Programm die Updates für Datenbanken und Module auf Ihren Computer herunterlädt.

KONTROLLIERTES OBJEKT

Datei, die mit den Protokollen HTTP, FTP oder SMTP übertragen und von der Firewall zur Untersuchung durch das Kaspersky-Lab-Programm umgeleitet wird.

KOPFZEILE (HEADER)

Informationen, die am Anfang einer Datei oder E-Mail stehen und Basisdaten über Status und Verarbeitung der Datei (E-Mail) enthalten. Die Kopfzeile einer E-Mail enthält z.B. Angaben über Absender, Empfänger und Datum.

L

LAUFWERKSBOOTSEKTOR

Ein Bootsektor ist ein spezieller Sektor auf der Festplatte eines Computers, auf einer Diskette oder auf einem anderen Gerät zur Datenspeicherung. Er enthält Angaben über das Dateisystem des Datenträgers und ein Bootprogramm, das für den Start des Betriebssystems verantwortlich ist.

Laufwerksbootsektoren können von so genannten Bootviren infiziert werden. Die Kaspersky-Lab-Anwendung erlaubt es, Bootsektoren auf Viren zu untersuchen und infizierte Sektoren zu desinfizieren.

LISTE DER VERTRAUENSWÜRDIGEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, deren Inhalt der Benutzer vertraut. Webseiten, die einem Element dieser Liste entsprechen, werden vom Kaspersky-Lab-Programm auf das Vorhandensein schädlicher Objekte nicht untersucht.

LISTE DER ZU UNTERSUCHENDEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, die vom Kaspersky-Lab-Programm auf das Vorhandensein schädlicher Objekte unbedingt untersucht werden sollen.

LISTE MIT ERLAUBTEN ABSENDERN

(auch weiße Adressenliste)

Liste mit E-Mail-Adressen. Die von diesen Adressen eintreffenden Nachrichten werden nicht vom Kaspersky-Lab-Programm untersucht.

LISTE MIT ERLAUBTEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, auf die der Zugriff vom Kaspersky-Lab-Programm nicht blockiert wird. Eine Adressenliste wird vom Benutzer bei der Programmkonfiguration erstellt.

LISTE MIT VERBOTENEN ABSENDERN

(auch schwarze Adressenliste)

Liste mit E-Mail-Adressen. Die von diesen Adressen eintreffenden Nachrichten werden vom Kaspersky-Lab-Programm ungeachtet ihres Inhalts blockiert .

LISTE MIT VERBOTENEN WEBADRESSEN

Eine Liste der Masken und Webressourcen, auf die der Zugriff vom Kaspersky-Lab-Programm blockiert wird. Eine Adressenliste wird vom Benutzer bei der Programmkonfiguration erstellt.

M

MAIL-DATENBANKEN

Datenbanken mit einem speziellen Format, in denen die auf Ihrem Computer gespeicherten E-Mails enthalten sind. Jede eingehende / ausgehende E-Mail wird nach dem Empfang / Senden in einer Mail-Datenbank gespeichert. Solche Datenbanken werden bei einer vollständigen Untersuchung des Computers untersucht.

Eingehende und ausgehende E-Mails werden im Augenblick des Empfangs und Sendens in Echtzeit auf Viren analysiert, wenn der Echtzeitschutz aktiviert ist.

MÖGLICHERWEISE INFIZIERTES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Infizierte Dateien können mit Hilfe der heuristischen Analyse gefunden werden.

N

NETZWERKPORT

Parameter für die Protokolle TCP und UDP, der den Zweck von Datenpaketen im IP-Format definiert, die über ein Netzwerk auf einen Host übertragen werden. Er erlaubt unterschiedlichen auf einem Host ausgeführten Programmen, unabhängig voneinander Daten zu empfangen. Jedes Programm verarbeitet die Daten, die auf einem bestimmten Port eintreffen (man sagt auch, ein Programm "hört" einen bestimmten Port).

Gewöhnlich sind häufig verwendeten Netzwerkprotokollen standardmäßige Portnummern zugeordnet (Webserver empfangen ihre Daten standardmäßig mit dem HTTP-Protokoll auf TCP-Port 80), obwohl ein Programm prinzipiell ein beliebiges Protokoll und einen beliebigen Port verwenden kann. Mögliche Werte: von 1 bis 65535.

O

OLE-OBJEKT

Objekt, das an eine andere Datei angehängt oder darin eingebettet ist. Das Kaspersky-Lab-Programm erlaubt es, OLE-Objekte auf das Vorhandensein von Viren zu untersuchen. Wenn Sie beispielsweise eine beliebige Tabelle aus Microsoft Office Excel in ein Dokument des Typs Microsoft Office Word einfügen, wird die Tabelle als OLE-Objekt untersucht.

OBJEKT BLOCKIEREN

Der Zugriff externer Programme auf ein Objekt wird verboten. Ein blockiertes Objekt kann nicht gelesen, ausgeführt, verändert oder gelöscht werden.

OBJEKT LÖSCHEN

Methode zur Objektbearbeitung, bei der das Objekt physikalisch von dem Ort gelöscht wird, an dem es vom Programm gefunden wurde (Festplatte, Ordner, Netzwerkressource). Diese Bearbeitungsmethode wird für gefährliche Objekte empfohlen, deren Desinfektion aus bestimmten Gründen nicht möglich ist.

OBJEKTE IN DIE QUARANTÄNE VERSCHIEBEN

Verarbeitungsmethode für ein möglicherweise infiziertes Objekt. Dabei wird der Zugriff auf das Objekt gesperrt und das Objekt wird vom ursprünglichen Speicherort in den Quarantäneordner verschoben. Dort wird es in verschlüsselter Form gespeichert, und eine Infektion wird dadurch ausgeschlossen.



PHISHING

Eine Art des Internetbetrugs, bei der E-Mails verschickt werden, um vertrauliche Informationen (i.d.R. finanziellen Charakters) zu stehlen.

POTENZIELL INFIZIERBARES OBJEKT

Ein Objekt das aufgrund seiner Struktur seines Formats von einem Angreifer als "Container" benutzt werden kann, um ein schädliches Objekt zu platzieren oder weiterzuverbreiten. In der Regel sind dies ausführbare Dateien mit Erweiterungen wie com, exe, dll usw. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

PRIORITÄTSSTUFE FÜR EIN EREIGNIS

Merkmale eines Ereignisses, das bei der Arbeit der Kaspersky-Lab-Anwendung eingetreten ist. Es gibt vier Prioritätsstufen:

Kritisches Ereignis.

Funktionsstörung.

Warnung.

Informative Meldung.

Ereignisse des gleichen Typs können unterschiedliche Prioritätsstufen besitzen. Entscheidend ist die Situation, in der ein Ereignis eintritt.

PROGRAMM AKTIVIEREN

Freischalten aller Programmfunktionen. Für die Aktivierung des Programms benötigt der Benutzer eine Lizenz.

PROGRAMM-MODULE

Dateien, die zum Lieferumfang von Kaspersky Lab gehören und für die Realisierung der wichtigsten Aufgaben zuständig sind. Jeder Art von Aufgaben, die das Programm realisiert (Echtzeitschutz, Virensuche, Update), entspricht ein eigenes ausführbares Modul. Wenn die vollständige Untersuchung Ihres Computers aus dem Hauptfenster gestartet wird, initiieren Sie den Start des Moduls für diese Aufgabe.

PROGRAMMEINSTELLUNGEN

Einstellungen für die Arbeit des Programms, die für alle Aufgabentypen gleich sind und sich auf das gesamte Programm beziehen (z.B. Leistungseinstellungen für das Programm, Einstellungen für Berichte, Backup-Einstellungen).

PROTOKOLL

Genau definierte und standardisierte Kombination von Regeln, die das Verhältnis zwischen Client und Server regulieren. Bekannte Protokolle und die entsprechenden Dienste sind z.B. HTTP (WWW), FTP und NNTP (News).

PROTOKOLLIERUNG

Aufzeichnung und Anzeige der Ergebnisse eines einzelnen Befehls bei der Ausführung des Programms im Debug-Modus.

PROXYSERVER

Dienst in Computernetzwerken, mit dem Clients indirekte Anfragen an andere Netzwerkdienste richten können. Zunächst baut der Client eine Verbindung zu einem Proxyserver auf und fragt nach einer bestimmten Ressource (zum Beispiel nach einer Datei), die auf einem anderen Server liegt. Dann stellt der Proxyserver mit dem angegebenen Server eine Verbindung her und nimmt von ihm die Ressource entgegen oder schreibt die Ressource in seinen eigenen Cache (falls der Proxy einen Cache besitzt). In einigen Fällen kann die Client-Anfrage oder Server-Antwort vom Proxyserver zu bestimmten Zwecken geändert werden.



QUARANTÄNE

Ein bestimmter Ordner, in den alle möglicherweise infizierten Objekte verschoben werden, die bei der Untersuchung oder im Rahmen des Echtzeitschutzes gefunden werden.

R

RESERVELIZENZ

Lizenz, die für die Arbeit der Kaspersky-Lab-Anwendung hinzugefügt, aber nicht aktiviert wurde. Eine Reservelizenz wird aktiviert, wenn die Gültigkeit der aktiven Lizenz abläuft.

RISIKOBEWERTUNG

Kennziffer für das Risiko, das ein Computerprogramm für das Betriebssystem darstellt. Die Bewertung erfolgt durch eine heuristische Analyse, die auf zweierlei Kriterien beruht:

statische Kriterien (z.B. Informationen über die ausführbare Programmdatei: Dateigröße, Erstellungsdatum usw.)

dynamische Kriterien, die dazu dienen, um die Arbeit des Programms in einer virtuellen Umgebung zu modellieren (Analyse der Aufrufe von Systemfunktionen durch das Programm).

Die Risikobewertung erlaubt es, für Schadprogramme typisches Verhalten zu erkennen. Je niedriger die Risikobewertung, desto mehr Aktionen werden einem Programm im System erlaubt.

ROOTKIT

Ein Programm oder ein Programmbausatz, dessen Ziel ist, die Spuren des Eindringlings zu verbergen oder die Anwesenheit der Malware im System zu verschleiern.

Unter Windows-Systemen mit Rootkit versteht man Software, die sich ins System einnistet und Systemfunktionen von Windows (Windows API) abfängt. Das Abfangen und die Modifizierung von Low-Level-API-Funktionen erlaubt solche Software ihr Vorhandensein im System gut zu maskieren. Unter anderem kann das Rootkit auch das Vorhandensein von vorgegebenen Objekten - zum Beispiel Prozesse, Ordner und Dateien auf der Festplatte, Registrierungsschlüssel - maskieren. Viele von Rootkits installieren ins System auch eigene Treiber und Dienste (diese sind auch "unsichtbar").



SOCKS

Proxyserver-Protokoll, mit dem eine zweiseitige Verbindung zwischen Computern eines lokalen und externen Netzwerks realisiert werden kann.

SCHLÜSSELDATEI

Datei mit der Endung key, die Ihr persönlicher "Schlüssel" ist und für die Arbeit mit einem Kaspersky-Lab-Programm erforderlich ist. Eine Schlüsseldatei ist im Lieferumfang des Produkts enthalten, wenn es bei einem Händler von

Kaspersky Lab erworben wurde, oder Sie erhalten sie per E-Mail, wenn das Produkt in einem Internet-Shop gekauft wurde.

SCHUTZSTATUS

Aktueller Schutzstatus, der das Sicherheitsniveau des Computers charakterisiert.

SCHWARZE LISTE FÜR SCHLÜSSELDATEIEN

Datenbank mit Informationen über die von Kaspersky Lab blockierten Schlüsseldateien. Die Datei mit der Schwarzen Liste wird gemeinsam mit den Datenbanken aktualisiert.

SCHWELLE FÜR VIRENAKTIVITÄT

Maximal zulässige Anzahl von Ereignissen eines bestimmten Typs innerhalb eines festgelegten Zeitraums, deren Überschreitung als erhöhte Virenaktivität und als Anzeichen eines Virenangriffs gilt. Dieser Wert besitzt insbesondere bei Viren-Epidemien große Bedeutung und erlaubt es dem Administrator, rechtzeitig auf drohende Virenangriffe zu reagieren.

SICHERHEITSSTUFE

Unter Sicherheitsstufe wird eine vordefinierte Auswahl von Parametern für die Arbeit einer Komponente verstanden.

SKRIPT

Ein kleines Computerprogramm oder ein unabhängiger Programmteil (Funktion), das/der in der Regel dazu dient, eine konkrete Aufgabe auszuführen. Meistens werden sie bei Programmen, die in Hypertext integriert sind, verwendet. Skripte werden beispielsweise gestartet, wenn Sie eine bestimmte Webseite öffnen.

Wenn der Echtzeitschutz aktiviert ist, überwacht die Anwendung den Start von Skripte, fängt sie ab und untersucht diese auf Viren. Abhängig von den Untersuchungsergebnissen können Sie die Ausführung eines Skripte verbieten oder erlauben.

SPAM

Unerwünschte massenhafte Versendung von E-Mails, die meistens Werbung enthalten.

SPEICHERDUMP

Inhalt des Speichers eines Prozesses bzw. des ganzen Arbeitsspeichers des Systems zu einem bestimmten Zeitpunkt.

SUBNETZMASKE

Die Subnetzmaske (auch Netzwerkmaske genannt) und die Netzwerkadresse definieren die Adressen der Computer, die zu einem Netzwerk gehören.

U

UND

UNBEKANNTER VIRUS

Neuer Virus, über den noch keine Informationen in den Datenbanken vorhanden sind. Unbekannte Viren werden mit der heuristischen Analyse erkannt und erhalten den Status möglicherweise infiziert.

UNTERSUCHUNG DES DATENVERKEHRS

Untersuchung von Objekten, die mit beliebigen Protokollen übertragen werden (z.B. HTTP, FTP u.a.). Die Untersuchung erfolgt im Echtzeitmodus unter Verwendung der aktuellen (letzten) Datenbankversion.

UPDATE

Vorgang, bei dem vorhandene Dateien (Datenbanken oder Programm-Module) durch neue Dateien ersetzt bzw. neue Dateien hinzugefügt werden. Die neuen Dateien werden von den Kaspersky-Lab-Updateservern heruntergeladen.

UPDATEPAKET

Dateipaket, das der Softwareaktualisierung dient, aus dem Internet kopiert und auf Ihrem Computer installiert wird.



VERDÄCHTIGE E-MAIL

E-Mail, die sich nicht eindeutig als Spam einstufen lässt, bei deren Untersuchung sich aber ein Verdacht ergeben hat (z.B. bestimmte Arten von Massenmails und Werbenachrichten).

VERDÄCHTIGES OBJEKT

Objekt, dessen Code entweder den modifizierten Code eines bekannten Virus oder einen Code, der einem Virus gleicht, enthält, der Kaspersky Lab aber bisher nicht bekannt ist. Verdächtige Objekte werden unter Einsatz der heuristischen Analyse erkannt.

VERFÜGBARES UPDATE

Updatepaket für die Module eines Kaspersky-Lab-Programms, das dringende Updates, die über einen bestimmten Zeitraum gesammelt wurden, sowie Änderungen der Programmarchitektur enthält.

VERTRAUENSWÜRDIGER PROZESS

Programmprozess, dessen Dateioperationen im Echtzeitschutz-Modus nicht von der Kaspersky-Lab-Anwendung kontrolliert werden. Das bedeutet, dass alle von einem vertrauenswürdigen Prozess gestarteten, geöffneten und gespeicherten Objekte nicht untersucht werden.

VIRENANGRIFF

Eine Reihe zielgerichteter Versuche, einen Computer mit einem Virus zu infizieren.



WIEDERHERSTELLUNG

Ein Originalobjekt wird aus der Quarantäne oder aus dem Backup entweder an den ursprünglichen Ort, an dem das Objekt gespeichert war, bevor es in die Quarantäne verschoben, desinfiziert oder gelöscht wurde, oder in einen benutzerdefinierten Ordner verschoben.

Z

ZERTIFIKAT DES ADMINISTRATIONSSERVERS

Zertifikat, mit dem der Administrationsserver beim Herstellen einer Verbindung mit der Administrationskonsole und Datenaustausch mit den Client-Computern authentifiziert wird. Das Zertifikat wird bei der Installation des Administrationsservers erstellt und auf dem Administrationsserver im Ordner %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert gespeichert.

KASPERSKY LAB

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor Viren und anderer Malware, Spam, Netzwerk- und Hackerangriffen schützen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach einer Studie des Marktforschungsinstituts COMCON TGI-Russia war Kaspersky Lab 2009 in Russland der beliebteste Hersteller von Schutzsystemen für Heimanwender.

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern mit Hauptsitz in Moskau und verfügt über fünf regionale Niederlassungen, die in Russland, West- und Osteuropa, im Nahen Osten, in Afrika, Nord- und Südamerika, Japan, China und anderen Ländern aktiv sind. Das Unternehmen beschäftigt über 2.000 hochspezialisierte Mitarbeiter.

Produkte. Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Antiviren-Anwendungen für Desktops, Laptops, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Programme und Services für den Schutz von Workstations, Datei- und Webservern, Mail-Gateways und Firewalls. In Verbindung mit Administrationstools ermöglichen es diese Lösungen, netzwerkweit einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen. Die Produkte von Kaspersky Lab sind durch namhafte Testlabore zertifiziert, mit den Programmen der meisten Softwarehersteller kompatibel und für die Arbeit mit unterschiedlichen Hardwareplattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Sie finden und analysieren jeden Tag Hunderte neuer Computerbedrohungen. Mit diesem Wissen entwickeln sie Mittel, um Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf die die Kaspersky-Programme zurückgreifen. *Die Antiviren-Datenbanken von Kaspersky Lab werden stündlich aktualisiert*, *die Anti-Spam-Datenbanken im 5-Minuten-Takt*.

Technologien. Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Softwarehersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (Großbritannien), CommuniGate Systems (USA), Critical Path (Irland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (Frankreich), NETGEAR (USA), Parallels (Russland), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

Auszeichnungen. Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So wurde Kaspersky Anti-Virus 2010 in Tests des anerkannten österreichischen Antiviren-Labors AV-Comparatives mehrfach mit dem Premium-Award Advanced+ ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 300 Millionen Anwender. Über 200.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Webseite von Kaspersky Lab:	www.kaspersky.de
Viren-Enzyklopädie:	http://www.securelist.com/de/
Antiviren-Labor:	newvirus@kaspersky.com (nur zum Einsenden von möglicherweise infizierten Dateien, die zuvor archiviert wurden) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=de (für Fragen an die Virenanalytiker)
Webforum von Kaspersky Lab:	http://forum.kaspersky.com

INFORMATIONEN ÜBER DEN CODE VON DRITTHERSTELLERN

Die Informationen über den Code von Drittherstellern sind in der Datei legal_notices.txt enthalten, die sich im Installationsordner des Programms befindet.

SACHREGISTER

A

B

D

E

N

P

Q

R

S

U

V

W

Z